The Implementation of Network-Centric Warfare

Office of Force Transformation

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
05 JAN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Implementation of Network-Centric Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Force Transformation,Office of the Secretary of Defense,1000 Defense Pentagon,Washington,DC,20301-1000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**82**	

Message from the Director, Office of Force Transformation

Warfare is about human behavior in a context of organized violence directed toward political ends. So, network-centric warfare (NCW) is about human behavior within a networked environment. "The network" is a noun, the information technology, and can only be the enabler. "To network" is the verb, the human behavior, the action, and the main focus. So, implementation of NCW must look beyond the acquisition of the technical enablers to individual and organizational behavior, e.g., organizational structure, processes, tactics, and the way choices are made. In other words, all elements of the enterprise are in play.

The U.S. Armed Forces' progress in transforming from the Industrial Age to the Information Age, though far from complete, has been illustrated during Operations Enduring Freedom and Iraqi Freedom. These campaigns, mounted against determined, potent foes in Afghanistan and Iraq, were characterized by the conduct of highly effective, network-centric operations by coalitions organized and led by the U.S. Central Command.

Our military is embracing NCW. All of the Service and Joint Transformation Roadmaps are based on a central principle. This is helping to create and maintain a decisive warfighting advantage for U.S. forces. In the Information Age, power is increasingly derived from information sharing, information access, and speed, all of which are facilitated by networked forces. NCW involves a new way of thinking about how we accomplish our missions and how we organize and interrelate within and among all echelons and at all levels of warfare—strategic, operational, and tactical.

Modern technology and new operational concepts enable networked units and individual platforms to operate together in ways not possible just a few years ago. NCW is characterized by the ability of geographically dispersed forces to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives in accordance with the commander's intent. This linking of people, platforms, weapons, sensors, and decision aids into a single network creates a whole that is clearly greater than the sum of its parts. The results are networked forces that operate with increased

speed and synchronization and are capable of achieving massed effects, in many situations, without the physical massing of forces required in the past. This increased speed and synchronization directly impacts operations across the battlespace, from support areas through combat zones.

In sum, NCW enhances the U.S. Armed Forces' ability to combine into a seamless, joint, coalition warfighting force. When implemented, it takes full advantage of the trust we place in our junior and noncommissioned officers. As information moves down echelon, so does decision making. Thus, smaller joint force packages can possess more flexibility and agility and are able to wield greater combat power than before. NCW generates new and extraordinary levels of operational effectiveness. It enables and leverages new military capabilities while allowing the United States and our multinational partners to use traditional capabilities with more speed and precision.

Recent progress in developing network-centric capabilities throughout the U.S. Armed Forces, evident in Afghanistan, Iraq, and elsewhere, is most encouraging, but we must not rest on our laurels. A great deal of work remains to be done. If we are to retain our competitive advantage in the 21st century, the Department must continue to move ahead in this vital area of military transformation.

How are the profound increases in capability and performance attributed to NCW implementation being attained from the perspective of force building and actual operations? This booklet will point to some of the answers.

A. K. Cebrowski
Director, Office of Force Transformation
Office of the Secretary of Defense

Contents

NCW Implementation

Conclusions—Network-Centric Warfare in Perspective

Introduction

"… we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace. Realizing these capabilities will require transforming our people, processes, and military forces."

Secretary of Defense Donald Rumsfeld,
Transformation Planning Guidance
April 2003

Introduction

Purpose

As the world enters a new millennium, our military simultaneously enters a new era in warfare—an era in which warfare is affected by a changing strategic environment and rapid technological change. The United States and our multinational partners are experiencing a transition from the Industrial Age to the Information Age. Simultaneously, we are fully engaged in a global war on terrorism set in a new period of globalization. These changes, as well as the experiences gained during recent and ongoing military operations, have resulted in the current drive to transform the force with network-centric warfare (NCW) as the centerpiece of this effort.

To better understand why NCW is so important to the force transformation process underway in the U.S. Armed Forces,[1] this document provides answers to some of the fundamental questions regarding NCW as an emerging theory of war in the Information Age. It also describes how the tenets and principles of NCW are providing the foundation for developing new warfighting concepts, organizations, and processes that will allow our forces to maintain a competitive advantage over potential adversaries, now and in the future. In sum, the purpose of this brochure is to provide an overview of the ongoing implementation of NCW in the Department of Defense (DoD).

A brief description of NCW, including its origins, its central role in force transformation, its tenets and principles, and an implementation strategy, are provided in this first chapter. An examination of NCW as an emerging theory of war, its relationship to the four domains of Information Age warfare, the growing evidence of its benefits, and the warfighting advantages it can provide, are examined in the second chapter. The third chapter focuses on network-centric operations (NCO), including the relationship of NCO to the overarching Joint Operations Concepts (JOpsC), the NCO experience in Afghanistan and Iraq, the development of the NCO Conceptual Framework, and the conduct of NCO case studies. An overview of Joint and Service plans and initiatives to develop and implement network-centric capabilities and the growing investment in these capabilities by our allies and multinational partners are provided in the fourth chapter.

What Is Network-Centric Warfare?

Network-centric warfare is an emerging theory of war in the Information Age. It is also a concept that, at the highest level, constitutes the military's response to the Information Age.[2] The term network-centric warfare broadly describes the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage.[3]

The implementation of NCW is first of all about human behavior as opposed to information technology. While "network" is a noun, "to network" is a verb. Thus, when we examine the degree to which a particular military organization, or the Department as a whole, is exploiting the power of NCW, our focus should be on human behavior in the networked environment. How do military forces behave, perform, and organize themselves when they are networked? As illustrated in the next chapter, experience with networked forces to date indicates that Soldiers, Sailors, Airmen, and

Marines conducting military operations at the tactical and operational levels of war gain a significant advantage over adversaries because of shared situational awareness. NCW theory has applicability at all three levels of warfare—strategic, operational, and tactical—and across the full range of military operations from major combat operations to stability and peacekeeping operations.

A networked force conducting network-centric operations (NCO) is an essential enabler for the conduct of effects-based operations by U.S. forces. Effects-based operations (EBO) are "sets of actions directed at shaping the behavior of friends, neutrals, and foes in peace, crisis, and war."[4] EBO is not a new form of warfighting, nor does it displace any of the currently recognized forms of warfare. Throughout history, decision makers have sought to create conditions that would achieve their objectives and policy goals. Military commanders and planners have attempted to plan and execute campaigns to create these conditions—an approach that would be considered "effects-based" in today's terminology. EBO in the 21st century, enabled by networked forces, is a methodology for planning, executing, and assessing military operations designed to attain specific effects that achieve desired national security outcomes.

The armed forces of many of our allies and multinational partners are moving rapidly into the NCW arena and developing network-centric capabilities of their own to be able to conduct EBO. When we conduct military operations with our allies and multinational partners today and in the future, we seek to obtain maximum advantage derived from the power of NCW. At the same time, it should not surprise us that our enemies and potential adversaries around the world, including international terrorist organizations like al Qaeda, may seek to acquire network-centric capabilities on their own terms in order to use them against us when conducting surveillance, planning operations, or actually carrying out attacks. It is reasonable to expect that terrorist organizations are also analyzing the vulnerabilities and weaknesses of our networks and planning to exploit them in the future.

NCW generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization **(figure 1)**. In essence, it

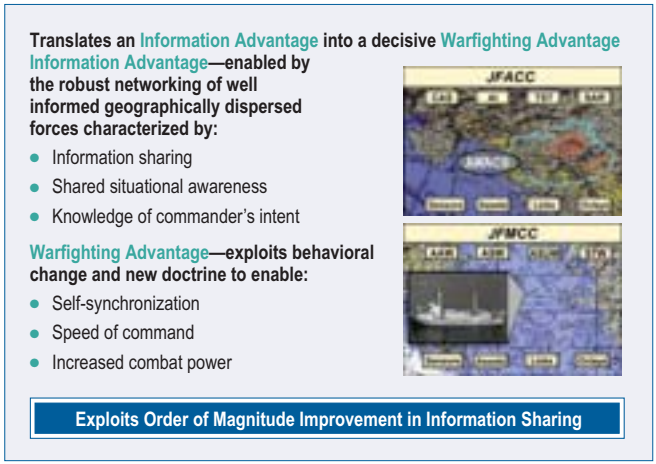


Figure 1: Information Age Transformation: Network-Centric Warfare

translates information advantage into combat power by effectively linking friendly forces within the battlespace, providing a much improved shared awareness of the situation, enabling more rapid and effective decision making at all levels of military operations, and thereby allowing for increased speed of execution. This "network" is underpinned by information technology systems, but is exploited by the Soldiers, Sailors, Airmen, and Marines that use the network and, at the same time, are part of it.

Origins of Network-Centric Warfare

One of the first clear, compelling descriptions of "network-centric warfare" was published in a 1998 *U.S. Naval Institute Proceedings* article. The authors compared the potential impact of NCW today with the transformational impact of the French concept of the *levee en masse* during the Napoleonic period. "NCW and all of its associated revolutions in military affairs (RMAs) grow out of and draw their power from the fundamental changes in American society. These changes have been dominated by the co-evolution of economics, information technology, and business processes and organizations and they are linked by three themes:

- The shift in focus from the platform to the network;
- The shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem; and
- The importance of making strategic choices to adapt or even survive in such changing ecosystems."[5]

These ideas have not only changed the nature of American business today—they have changed and will continue to change the way military operations are conducted.

The development of the intellectual foundation of NCW within the DoD continued with the Information Age Transformation Series of books published by the Department of Defense Command and Control Research Program (CCRP) under the auspices of the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]). The first book in this series, *Network Centric Warfare: Developing and Leveraging Information Superiority*, provided the first detailed articulation of the tenets that link a robustly networked force to dramatically increased combat power.[6] It also described how information, coupled with changes in command and control (C2), could transform military organizations. Two additional volumes completed the three-volume set, *Information Age Anthology: Understanding Information Age Warfare* and *Information Age Transformation.*[7] Another important book published by the CCRP, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis and War*, explored the link between network-centric organizations and processes and mission outcomes.[8]

Central Role in Force Transformation

The President and the Secretary of Defense have frequently emphasized that the transformation of the Department of Defense lies at the heart of U.S. defense strategy. As one of the seven major interconnected tenets of our strategy, transformation supports the four major defense policy goals: assuring allies and friends; dissuading future military competition; deterring threats and coercion against U.S. interests; and, if deterrence fails, decisively defeating any adversary.

Overall, DoD's transformation addresses three major areas—how we do business inside the Department, how we work with our interagency and multinational partners, and how we fight. While all three areas are vital in the Department's ongoing transformation to the Information Age, the concepts of NCW and our steadily improving network-centric capabilities are transforming how we fight. Thus, NCW is at the very center of force transformation.

Force transformation includes new technologies but also depends on the development of new operational concepts, organizational structures, and relationships. The development of network-centric capabilities depends on all of these. The ongoing shift from platform-centric to network-centric thinking and NCW is key to force transformation and an evolving approach to the conduct of joint warfare in the Information Age.[9]

The development of network-centric organizations and the growing capability of U.S. forces to conduct NCO are not ends in themselves, but a means to generate increased combat power by:

- Better synchronizing events and their consequences in the battlespace;
- Achieving greater speed of command; and
- Increasing lethality, survivability, and responsiveness.

As already mentioned, the capability to conduct NCO is a key enabler of effects-based operations (EBO). Unless our forces are able to apply their network-centric capabilities to achieve the effects that result in attaining strategic, operational, or tactical objectives, the full value of these capabilities will not be realized. In addition, without a robust network structure and the phenomena that result from the application of network-centric capabilities, it will be far more difficult, if not impossible, for the U.S. and our multinational partners to conduct NCO and EBO against our adversaries.

"Throughout history, warfare has assumed the characteristics of its age and the technology of its age. Today we see this trend continuing as we move from the Industrial Age warfare with its emphasis on mass to Information Age warfare, which highlights the power of networked distributed forces and shared situational awareness … Within this wider context of military transformation, network-centric warfare is one of the key concepts for thinking about how we will operate in the future."

Deputy Secretary of Defense Paul Wolfowitz, July 2001.

Tenets and Principles of Network-Centric Warfare

Four basic tenets of NCW and a set of governing principles for a network-centric force have been identified. Together, these tenets and principles comprise the core of NCW as an emerging theory of war in the Information Age. The four tenets of NCW help us understand the enhanced power of networked forces. At the same time, they constitute a working hypothesis about NCW as a source of warfighting advantage:

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- These, in turn, dramatically increase mission effectiveness.[10]

The governing principles for a network-centric force are summarized in **figure 2** and discussed in more detail below. These principles, still evolving and subject to further refinement, are guiding the application of NCW as an emerging theory of war. In effect, they constitute the new rules by which a network-centric force organizes, trains, and operates.

Governing Principles

- Fight first for ***information superiority***
- Access to information: ***shared awareness***
- ***Speed of command*** and decision making
- ***Self-synchronization***
- ***Dispersed forces:*** non-contiguous operations
- ***Demassification***
- ***Deep sensor reach***
- ***Alter initial conditions*** at higher rates of change
- ***Compressed operations*** and levels of war

Figure 2: Governing Principles of a Network-Centric Force

While it is not suggested that the governing principles for a network-centric force have supplanted or are going to replace the time-tested principles of war—mass, objective, offensive, security, economy of force, maneuver, unity of command, surprise, simplicity—they provide added direction for executing military operations in the Information Age. They are guiding the development and refinement of the overarching JOpsC and the four subordinate Joint Operating Concepts (JOC): Homeland Security; Major Combat Operations; Stability Operations; and Strategic Deterrence.

Fight First for Information Superiority: Generate an information advantage through better timeliness, accuracy, and relevance of information.

- Increase an enemy's information needs, reduce his ability to access information, and raise his uncertainty.
- Assure our own information access through a well networked and interoperable force and protection of our information systems, including sensor systems.
- Decrease our own information needs, especially in volume, by increasing our ability to exploit all of our collectors.

Shared Awareness: Routinely translate information and knowledge into the requisite level of common understanding and situational awareness across the spectrum of participants in joint and combined operations.

- Build a collaborative network of networks, populated and refreshed with quality intelligence and non-intelligence data, both raw and processed, to enable forces to build a shared awareness relevant to their needs.
- Information users must also become information suppliers, responsible for posting information without delay. Allow access to the data regardless of location.
- High-quality shared awareness requires secure and assured networks and information that can be defended.

Speed of Command and Decision Making: Recognize an information advantage and convert it into a competitive advantage by creating processes and procedures otherwise impossible (within prudent risk).

- Through battlefield innovation and adaptation, compress decision timelines to turn information advantage into decision superiority and decisive effects.
- Progressively lock out an adversary's options and ultimately achieve option dominance.

Self-Synchronization: Increase the opportunity for low-level forces to operate nearly autonomously and to re-task themselves through exploitation of shared awareness and the commander's intent.

- Increase the value of subordinate initiative to produce a meaningful increase in operational tempo and responsiveness.
- Assist in the execution of the "commander's intent." Exploit the advantages of a highly trained, professional force.
- Rapidly adapt when important developments occur in the battlespace and eliminate the step function character of traditional military operations.

Dispersed Forces: Move combat power from the linear battlespace to non-contiguous operations.

- Emphasize functional control vice physical occupation of the battlespace and generate effective combat power at the proper time and place.
- Be non-linear in both time and space, but achieve the requisite density of power on demand.
- Increase close coupling of intelligence, operations, and logistics to achieve precise effects and gain temporal advantage with dispersed forces.

Demassification: Move from an approach based on geographically contiguous massing of forces to one based upon achieving effects.

- Use information to achieve desired effects, limiting the need to mass physical forces within a specific geographical location.
- Increase the tempo and speed of movement throughout the battlespace to complicate an opponent's targeting problem.

Deep Sensor Reach: Expand use of deployable, distributed, and networked sensors, both distant and proximate, that detect actionable information on items of interest at operationally relevant ranges to achieve decisive effects.

- Leverage increasingly persistent intelligence, surveillance, and reconnaissance (ISR).
- Use sensors as a maneuver element to gain and maintain information superiority.
- Exploit sensors as a deterrent when employed visibly as part of an overt display of intent.
- Enable every weapon platform to be a sensor, from the individual soldier to a satellite.

Alter Initial Conditions at Higher Rates of Change: Exploit the principles of high-quality shared awareness, dynamic self-synchronization, dispersed and de-massed forces, deep sensor reach, compressed operations and levels of war, and rapid speed of command to enable the joint force to swiftly identify, adapt to, and change an opponent's operating context to our advantage. Warfare is highly path-dependent; hence, the imperative to control the initial conditions. The close coupling in time of critical events has been shown historically to have profound impact both psychologically and in locking out potential responses.

Compressed Operations and Levels of War: Eliminate procedural boundaries between Services and within processes so that joint operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects.

- Increase the convergence in speed of deployment, speed of employment, and speed of sustainment.
- Eliminate the compartmentalization of processes (e.g., organize, deploy, employ, and sustain) and functional areas (e.g., operations, intelligence, and logistics).
- Eliminate structural boundaries to merge capabilities at the lowest possible organizational levels, e.g., joint operations at the company/sub-squadron/task unit level.

Strategy for Implementation

The Department's overall strategy for NCW implementation is based upon: 1) Setting priorities to enable, develop, and implement network-centric concepts and capabilities; 2) Establishing specific goals and measuring progress toward these goals; and 3) Overcoming impediments to progress.

Setting Priorities: A critical mass of the Joint Force must be robustly networked as the "entry fee" for NCW and transformation. This requires a focus on interoperability which must not be sacrificed for near-term considerations. Battlespace entities (platforms, units, sensors, shooters) must be designed "net-ready." In addition, increased emphasis must be placed upon research in developing shared situational awareness and new organizational approaches to achieving synchronization. Research must continue to improve our ability to accurately represent NCW-related concepts and capabilities in models and simulations and to help us understand and manage complex networks.

Establishing Goals and Measuring Progress: The Department recognizes the need to establish measurable NCW goals, to develop an investment and implementation plan to achieve these goals, and to measure progress. An immediate goal must be the availability of a robustly networked joint force that can experiment with network-centric concepts and capabilities accompanied by a campaign of experimentation focused on discovery. To measure progress, metrics are needed. Ongoing efforts to develop measures of key aspects of NCW, including the quality of information, collaboration, awareness, and shared situational awareness, have been given more emphasis and related to measures of command and control, synchronization, and, ultimately, to measures of mission effectiveness.

Overcoming Impediments to Progress: Technical, cultural, and organizational impediments to accelerating the Department's progress in fully implementing NCW remain. Each can be overcome through focused efforts in areas such as network security, network interoperability, an understanding of human and organizational behavior, and key NCW-enabling technologies. The creation of a DoD environment that supports innovation will enable us to reap the full potential of NCW, just as better understanding of individual, team, organizational, and cultural behaviors will significantly accelerate our progress in implementing NCW.[11]

Key Elements of Proposed NCW Implementation Strategy: The DoD strategy for the implementation of NCW includes seven key elements:[12]

- **Get the Theory Right:** The new rules of Information Age warfare and the theory of NCW must be continually refined through the process of experimentation and testing and from the real world experience of U.S. forces engaged in combat and other military operations worldwide, including ongoing stability operations in Afghanistan, Iraq, Kosovo, and Bosnia.
- **Apply the Theory Enterprise Wide:** It will not be enough to implement network-centric capabilities, conduct network-centric operations (NCO), and test the theory of NCW only in a "critical mass of the joint force" or in certain high priority units. Instead, the capabilities must be developed and the theory applied enterprise wide, i.e., throughout the DoD.

- **Accelerate Networking of the Joint Force:** Understandably, much of the effort to network U.S. forces to date has been undertaken by the Services. In the future, however, joint forces must be networked not only at the strategic and operational levels, but also at the tactical level.

- **Accelerate Deployment of Network-Centric Systems, Concepts, and Capabilities:** As new network-centric systems, concepts, and capabilities are developed by the Services and Combatant Commands, they should be deployed to the units and geographical areas where they can be refined and employed when needed.

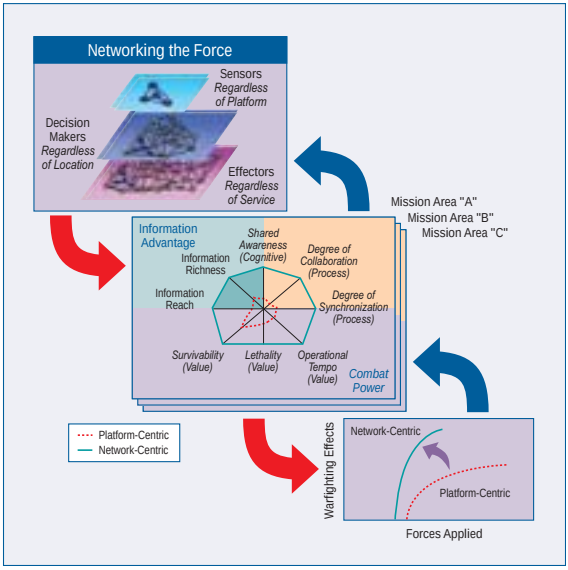


Figure 3: Applying NCW Theory to Support Key Force Development and Investment Decisions

- **Experiment with Network-Centric Concepts and Capabilities:** The role of experimentation in advancing the implementation of network-centric concepts and capabilities is absolutely critical. The Department depends upon a rigorous program of Joint and Service experimentation to nurture new and better ways to conduct NCO.

- **Address Challenges of Allied and Coalition NCO:** As discussed in the third chapter, U.S. allies and multinational partners are developing their own concepts and capabilities for the conduct of NCO. Some of the challenges of conducting NCO within the NATO alliance have already surfaced during operations in Bosnia and Kosovo and to some extent in Afghanistan and Iraq. These challenges should be addressed and overcome as soon as possible.

- **Develop Doctrine and Tactics, Techniques, and Procedures (TTP) for NCO:** In order to maximize the potential for increased combat power from NCW, Joint and Service warfighting doctrines must evolve as network-centric capabilities are implemented in U.S. forces. Simultaneously, mature TTPs will be needed to facilitate the effective conduct of NCO by U.S., allied, and multinational forces during combined military operations.

The Department's strategy for implementing NCW, as outlined above, is having a major impact on key force development and investment decisions by the Department and the Services. **Figure 3** illustrates how the application of NCW theory can support key DoD investment decisions.

Theory and Practice of Network-Centric Warfare

"What we are seeing, in moving from the Industrial Age to the Information Age, is what amounts to a new theory of war: power comes from a different place, it is used in different ways, it achieves different effects than it did before. During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed. We have come to call that new theory of war network-centric warfare. It is not only about networks, but also about how wars are fought—how power is developed."

Vice Admiral (Ret.) Arthur K. Cebrowski,
Director, Office of Force Transformation,
IEEE Spectrum,
July 2002.

Theory and Practice of Network-Centric Warfare

An Emerging Theory of War

A theory is "a hypothesis assumed for the sake of argument or investigation, an unproved assumption."[13] It is also "a formulation of apparent relationships or underlying principles of certain observed phenomena which has been verified to some degree."[14] The working hypothesis of network-centric warfare (NCW) as an emerging theory of war, simply stated, is that the behavior of forces, i.e. their choices of organizational relationships and processes, when in the networked condition, will outperform forces that are not. The four basic tenets of NCW, introduced in the preceding chapter, elaborate on this basic premise. The governing principles of a network-centric force guide the application of this emerging theory of war and help to explain its power.

A theory of war must account for new sources of power, relations among them, and how they are brought to bear across the entire spectrum of military competition from peacekeeping, deterrence, and dissuasion to violent clashes and sustained, high-intensity conflict, and from force building and countering traditional threats to countering irregular, catastrophic, and disruptive threats. The basis of NCW as an emerging theory of war is that power flows from society and society's methods of creating power and wealth and that there has been a fundamental shift in sources of power from industry to information. This is comparable to the earlier shift from the Agrarian Age to the Industrial Age. In the Industrial Age, land was still important, but it was no longer the primary source of power and wealth. In the Information Age, industrial power remains important, but it has been replaced by information as the most important source of power and wealth. NCW is in a different competitive space from Industrial Age warfare and, therefore, has some different competitive attributes.

NCW is an emerging theory of war because it identifies new sources of power (information sharing, information access, speed), how those sources relate to each other, how they are brought to bear to gain the desired outcome, and how they link to political objectives **(figure 4)**. It explains how one side uses violence to compel an opponent to do what it would not otherwise do and eliminate the opponent's ability to do the same to them. It speaks to the character of war, not to its nature, accepting that war by nature is a form of intense human competition and involves violence, profound risk, and mutual danger. The NCW emerging theory of war accepts the notion that it is the nature of war to be nasty, brutish, and very complex, however short a conflict, campaign, or battle may be. Some have said that NCW applies only to "high-end" traditional warfare. This says more

Figure 4: Network-Centric Warfare … An Emerging Theory of War

about our preference for "high-end" traditional warfare than it does about NCW, an emerging theory of war that applies to all levels and modes of competition.

Many of the recent and ongoing efforts to enhance the network-centric capabilities of U.S. forces have focused on the tactical and operational levels of war. However, the relevance of NCW extends to the strategic level. Strategy involves choices that control the scope, pace, and intensity of a conflict. As shown during the major combat operations phase of Operation Iraqi Freedom, the capabilities of the forces in the networked environment gave senior civilian leaders a broader array of options not otherwise possible.

As with other, earlier theories of war[15], NCW has its competitive space, rule sets, and metrics. Where the competitive space of industrial warfare was the capacity to produce heavy weapons and get them to where they could be most destructive, the competitive space in NCW is the capability to obtain and integrate information into military operations. The metrics used to gauge the relative power of military forces in the Industrial Age were generally input measures. We measured and compared military mass, expressed in terms of numbers of weapons, ton-miles per day, military manpower, and units. Our planning focused on achieving a superior advantage in each of these areas, whether in individual battles or larger campaigns. But the metrics of NCW seek to describe the relative ability to create an information advantage and turn it into a military advantage. These metrics are generally output measures like speed, rates of change, operational and tactical innovation, how fast one side can couple events together and act on the information, and achieve political outcomes.

Where Industrial Age warfare revolved around efforts to obtain overwhelming force and attrition, NCW revolves around information superiority[16] and precision violence to dismantle an opposing force.

Assuming NCW gains wide acceptance as a new or emerging theory of war, is it likely to render the works of Carl von Clausewitz and other classical strategic thinkers obsolete? Michael Handel of the Naval War College, one of the foremost contemporary students of Clausewitz, Sun Tzu, Mao Tse-tung, Jomini, and others, concluded that while the classic strategic theories of war may require adaptation to a changing environment such as we are experiencing in the Information Age and in the conduct of the global war on terror, they remain fundamentally intact. The logic of waging war and of strategic thinking is as universal and timeless as human nature itself.

Observing that for many students of war today, "the advantages offered by advanced military technology represent the realization of a long-awaited panacea for the complex political and strategic problems of waging war," Handel adds a useful note of caution for those involved in the implementation of NCW. "Many of the latest military theories and doctrines assume tacitly or explicitly that the wars of the future will be waged with perfect or nearly perfect information and intelligence ('information dominance') … This vision is a chimera, because it implies that friction in war will be greatly reduced if not eliminated."[17] This will not be the case. Rather, the issue is how one creates and exploits an information advantage within the context of the fog and friction of war.

A survey of recent and emerging military theories and the future of war has led to the observation that, "In the 1990s, military theory reflected the rapid diffusion of conflict following the end of the bipolar Cold War world." These theories ranged from John Mueller's "obsolescence of major war" theory and Martin van Creveld's argument that Western military theory derived from classical warfare had become obsolescent to Alvin and Heidi Toffler's theory of "third wave" high-technology information warfare. According to the Tofflers and the Information Age theorists who followed them, the Gulf War of 1990–91 had provided a glimpse of postmodern war as the realm of high technology. On the other hand, military writers like Ralph Peters, Robert Kaplan, and Philip Cerny have offered visions of future war involving the "coming anarchy" of a world of failed states or a struggle by the West against a world of warrior cultures and paramilitaries. The intellectual challenge facing military professionals in the early 21st century is not, as some are suggesting, "to consign Carl von Clausewitz to the dustbin of history. Rather the task is to learn how to fight effectively across the spectrum of conflict."[18] The NCW theory of war, as it is implemented throughout the U.S. Armed Forces, addresses this formidable task.

Information Age Warfare

Network-centric warfare (NCW) offers a unique approach to the conduct of joint warfare in the Information Age. Constructed around the tenets of NCW and the governing principles of a network-centric force and emphasizing high-quality shared awareness, dispersed forces, speed of command, and flexibility in planning and execution, the application of this emerging theory of war is giving U.S. forces the capability to conduct immensely powerful effects-based operations (EBO) to achieve strategic, operational, and tactical objectives across the full range of military operations.

The recent performance of U.S. forces in the successful conduct of Operations Enduring Freedom (OEF, Afghanistan, 2001–2002) and Iraqi Freedom (OIF, Iraq, 2003) has provided a glimpse of its potential. As General Tommy Franks, USA (Ret.), commander of coalition forces during OEF and OIF, observed recently, "I believe one of the lessons well identified as enduring is the power of a net-centric approach, which [lends itself] to the effects of munitions, actions, and information rather than the old way of stove-piping activities." When reflecting on OIF and his ability to see the accurate locations of his forces in near-real-time, thanks to the Blue Force Tracking (BFT) system

used by ground forces, General Franks described his feelings at the time: "… I've died and gone to heaven and seen the first bit of net-centric warfare at work!"[19]

Information technology advances in the areas of command and control (C2); intelligence, surveillance, and reconnaissance (ISR); and precision weapons delivery are dramatically reshaping the conduct of warfare in the 21st century, as General Franks and many others witnessed in Afghanistan and Iraq. The principles of NCW provide a new foundation with which to examine and consider changes in military missions, operations, and organizations in the Information Age. The full application of these principles will accelerate the decision cycle by linking sensors, communications networks, and weapons systems via an interconnected grid, thereby enhancing our ability to achieve information and decision superiority over an adversary during the conduct of military operations.

As a new source of power, NCW has a profound impact on the planning and conduct of war by allowing forces to increase the pace and quality of decision making, in effect changing the rules and pace of military operations. A warfighting force with networked capabilities allows a commander to more quickly develop situational awareness and understanding, rapidly communicate critical information to friendly combat forces, and marshal the appropriate capabilities to exert massed effects against an adversary.

As mentioned previously, NCW provides the foundation for transforming the way U.S. forces will organize and fight in the Information Age. While NCW is the theory, network-centric operations (NCO) is the theory put into action. In other words, the conduct of NCO represents the implementation of NCW. Military operations will emphasize gaining and maintaining information superiority to provide a competitive advantage based on the implementation of NCW and its principles. The objective of decision superiority is to turn an information advantage into a competitive advantage.

"Information Superiority is an imbalance in one's favor in the information domain with respect to an adversary. The power of superiority in the information domain mandates that the United States fight for it as a first priority even before hostilities begin … The quality of the information position depends on the accuracy, timeliness, and relevance of information from all sources … The continuous sharing of information from a variety of sources enables the fully networked Joint Force to achieve the shared situational awareness necessary for decision superiority."

Department of Defense, Joint Operations Concepts, November 2003, p. 17.

This competitive advantage is readily apparent when comparing forces conducting NCO and those operating under the old paradigm of platform-centric operations. Platform-centric forces lack the ability to leverage the synergies created through a networked force. A force implementing NCW is more adaptive, ready to respond to uncertainty in the very dynamic environment of the future at all levels of warfare and across the range of military operations. When we consider the most recent combat experience of U.S. forces in Afghanistan and Iraq, it is apparent that platforms retained a central focus, but the networking of those platforms and organizations greatly enhanced their lethality and survivability.

Network-Centric Warfare and the Domains of Conflict

To successfully implement the emerging theory of war and the NCW capabilities now being developed by the U.S. and our multinational partners, the four domains of warfare—physical, information, cognitive, and social—must be understood, as well as the intersections, or areas of overlap, between the domains. As stated earlier, the four basic tenets of NCW constitute a hypothesis regarding NCW as a source of power. **Figure 5** illustrates how this hypothesis may be explored at a high level across the domains of Information Age warfare.

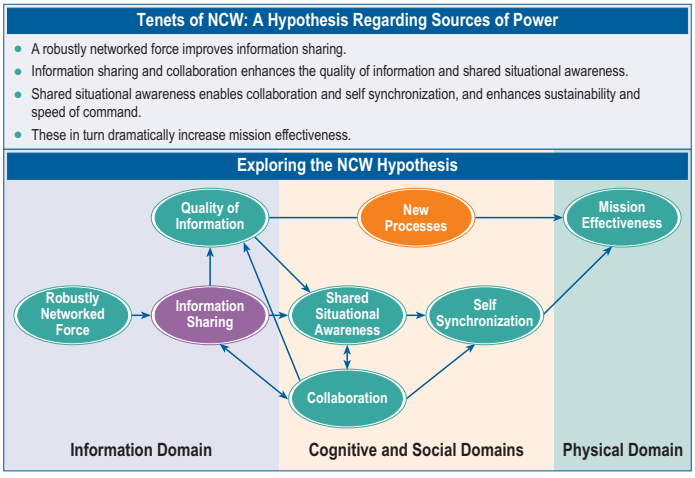


Figure 5: Tenets of NCW … the New Value Chain

The overarching Joint Operations Concepts (JOpsC) and its subordinate Joint Operating Concepts (JOCs), Joint Functional Concepts (JFCs), Joint Integrating Concepts (JICs), architectures, requirements, and capabilities are based upon the vision of a transforming network-centric joint force and a capabilities-based defense strategy designed to attain the six operational goals established by the Secretary of Defense in the 2001 Quadrennial Defense Review.

The required attributes and capabilities of a new joint force capable of conducting NCO must be carefully considered for each of these four domains.

Physical Domain: The physical domain is the traditional domain of warfare where a force is moved through time and space. It spans the land, sea, air, and space environments where military forces execute the range of military operations and where the physical platforms and communications networks that connect them reside. Comparatively, the elements of this domain are the easiest to measure and, consequently, combat power has traditionally been measured in the physical domain.

Information Domain: The information domain is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. This is the domain of sensors and the processes for sharing and accessing sensor products as well as "finished" intelligence. It is where C2 of military forces is communicated and the commander's intent is conveyed. Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions by an adversary.

Cognitive Domain: The cognitive domain is in the mind of the warfighter. This is the realm of EBO. Many, though not all, battles, campaigns, and wars are won in this domain. The intangibles of leadership, morale, unit cohesion, level of training and experience, and situational awareness are elements of this domain. This is the domain where commander's intent, doctrine, tactics, techniques, and procedures reside. This is also where decisive battlespace concepts and tactics emerge.

Social Domain: The social domain describes the necessary elements of any human enterprise. It is where humans interact, exchange information, form shared awareness and understandings, and make collaborative decisions. This is also the domain of culture, the set of values, attitudes, and beliefs held and conveyed by leaders to the society, whether military or civil. It overlaps with the information and cognitive domains, but is distinct from both. Cognitive activities by their nature are individualistic; they occur in the minds of individuals. However, shared sensemaking—the process of going from shared awareness to shared understanding to collaborative decision making—is a socio-cognitive activity because the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa.[20]

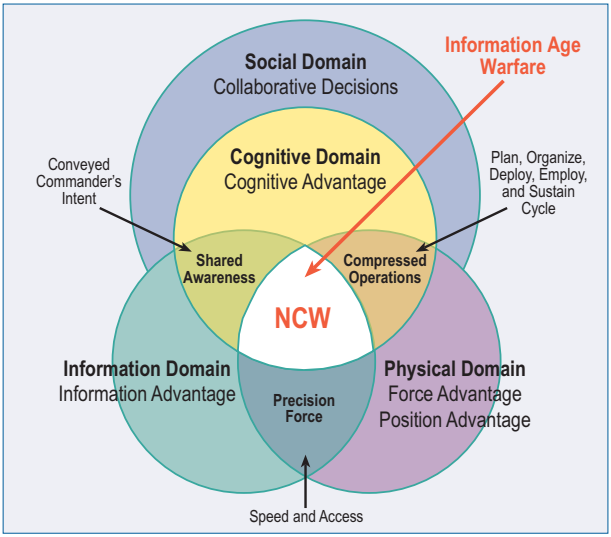


Figure 6: Information Age Warfare … Domains of Conflict

As illustrated in **figure 6,** the domain intersections represent important, dynamic areas within which concept-focused experimentation should be conducted. The precision force so vital to the conduct of successful joint operations is created at the intersection of the information and physical domains. Shared awareness and tactical innovation occur at the intersection between the information and cognitive domains. Since many battles and campaigns are actually won or lost in the cognitive domain, this intersection is enormously important. The intersection between the physical and cognitive domains is where the time compression and "lock-out" phenomenon occur, where tactics achieve operational and even strategic effects, and where high rates of change are developed. NCW exists at the very center where all four domains intersect.

Benefits of Network-Centric Warfare

Evidence accumulated from a wide range of U.S. military activities, including combat operations, training events, exercises, and demonstrations, has strongly supported the validity of NCW as an emerging theory of war and illustrated the power of networked forces. In general, the outcomes have consistently been decisive in favor of forces that are robustly networked. When both sides have similar networking capabilities, competition shifts to other attributes. This is discussed further in the final chapter, "Conclusions—Network-Centric Warfare in Perspective."

In some tactical engagements, "superior" platforms were decisively defeated by "less capable" platforms that were able to leverage order-of-magnitude improvements in information sharing enabled by networking. In other engagements, digitized and networked ground forces with a reduced number of "platforms" were able to "substitute information for mass" and outperform units equipped with a larger number of "platforms" not similarly digitized and networked. Even more impressively, the combination of networked and digitized ground and air forces was able to decisively defeat an opposition force (OPFOR) with unprecedented lethality by creating and leveraging an information advantage.

Air-to-Air Mission Area: Some of the most thoroughly documented and convincing examples of the power of NCW have been drawn from the air-to-air mission area. Increased situational awareness and enhanced situational understanding are major contributors to enhanced survivability and lethality in this mission area. With audio-only communications, pilots and controllers must share information on adversary forces generated by onboard sensors, as well as their own position and status, via voice. Communicating the minimum essential information by voice takes time and the resulting situational awareness often differs significantly from reality.

In contrast, when datalinks are employed on fighter aircraft, digital information on blue and red forces is shared instantaneously, enabling all participants to share a common tactical picture. This improved information position constitutes a significant "information advantage" as compared to an adversary fighting with only voice communications. This information advantage, in turn, enables a cognitive advantage, in the form of dramatically increased shared situational awareness and enhanced situational understanding. The result is that pilots flying datalink-equipped aircraft can translate these advantages into increased survivability and lethality.[21]

The same sort of evidence of increased warfighting effectiveness enabled by networking during air-to-air combat has been demonstrated in other important mission areas including combined arms maneuver warfare and close air support (Division Capstone Exercise—Phase I); counter anti-access (Fleet Battle Experiment Foxtrot); counter-special operations forces (SOF) (Fleet Battle Experiment Delta); and multinational rapid reaction forces (Allied Command Europe Mobile Force—Land) **(figure 7)**.

Combined Arms Maneuver and Close Air Support: One of the most powerful, well documented examples of increased warfighting advantage achieved through NCW was provided by the U.S. Army's Division Capstone Exercise—Phase I (DCX-1), conducted in the spring of 2001 at the National Training Center at Ft. Irwin, California. During this exercise, the Blue Force, consisting of two brigade combat teams (BCT) of the 4th Infantry Division with close air support (CAS) provided by F-16 and A/OA-10s from the Arizona Air National Guard, was digitized and networked to a degree never before achieved in a major joint exercise.

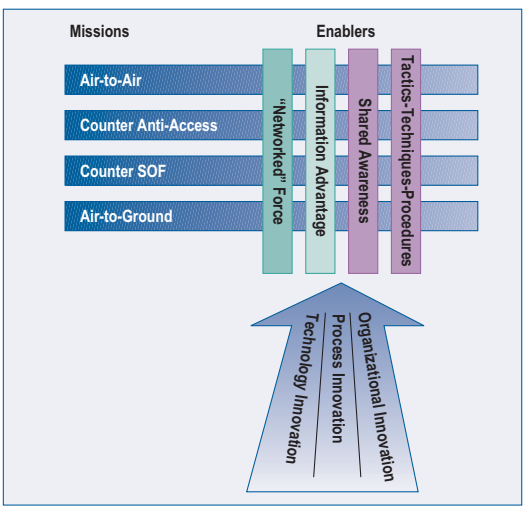


Figure 7: Understanding the Evidence for NCW Warfighting Advantage

During DCX-1, digitized and networked forces demonstrated significantly improved warfighting capabilities and prevailed over the opposing force (OPFOR) in multiple engagements. The Arizona Air National Guard F-16s and A/OA-10s providing CAS to the ground forces were equipped with the Situational Awareness Data Link (SADL), enabling them to exchange real-time targeting information and receive a current forward trace of the Blue Forces on the ground situation. The result of this networking was more than an order-of-magnitude improvement in the ability of ground and air forces to work together through more effective sharing of information.[22] As a direct result, the networked joint force employing combined arms maneuver during DCX-1 decisively defeated an experienced, well-trained OPFOR **(figure 8)**.

In the words of a mechanized infantry company commander whose unit participated in DCX-1, "When fighting at night, these systems are unmatched. My Bradleys made direct fire kills routinely at 3700 meters and beyond. Additionally, the FBCB2 increased our situational awareness dramatically. We were able to conduct bold maneuvers at night that we would normally only do during daylight."[23]

A Source of Warfighting Advantage

Over thousands of years of recorded history, the vast majority of innovations that created significant warfighting advantages were concentrated in the physical domain as opposed to the information domain. These innovations translated primarily into advantages at the tactical level of warfare, but they also had an impact on what are now generally referred to as the operational and strategic levels of warfare. They resulted in such battlefield advantages as: increased range of engagement (composite bow, rifled musket, long-range artillery, long-range bombers, guided and ballistic missiles); increased lethality (gunpowder, musket, rifle, machine gun, rocket launcher, chemical warhead, nuclear weapon); increased speed of maneuver (chariot, horse cavalry, steam propulsion for ships, railroads, combustion engine, tanks, jet engine, nuclear propulsion); and increased protection and survivability (body armor, fortifications, trench warfare, battleships, submarines, tanks, armored personnel carriers, armored fighting vehicles, low observable "stealthy" aircraft and ships).

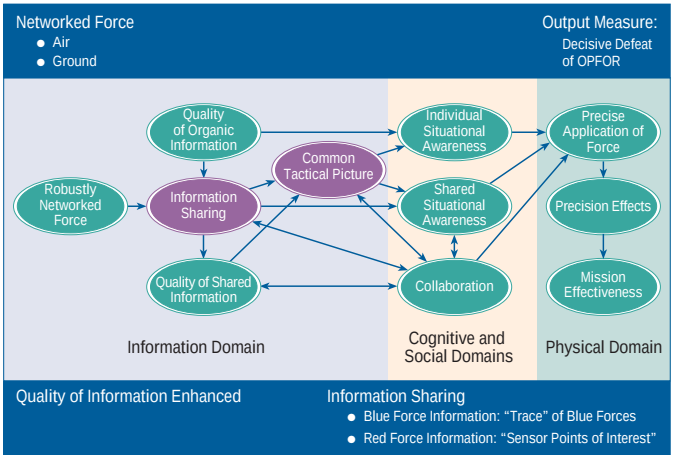


Figure 8: Exploiting Order of Magnitude Change (DCX-1)

While all of these examples of innovation are considered platform-centric, the past century has also

Figure 9: OIF Screen Capture – Common Operational Picture

seen many innovations focused on creating advantage in the information domain. The ability to develop and exploit an information advantage has always been important in warfare, hence the timelessness of security and surprise as important principles of war. Examples of innovations that created information advantages in warfare have included couriers on horseback, signal flags, encryption and code breaking, telegraph, wireless radio, aerial reconnaissance and photography, radar, electronic warfare, satellites (communications, reconnaissance), and advances in navigation (magnetic compass, Global Positioning System [GPS]). While the importance of innovation in the information domain in the past has been great, its importance has gained critical significance in warfare today.

Today, the implementation of NCW through the conduct of NCO is creating a warfighting advantage for those who pursue it. At the most basic level of warfare, there has always been a critical need to be able to distinguish friend from foe on the battlefield, day and night and in all sorts of terrain and weather conditions. The introduction and widespread use of night vision equipment has provided our forces with a very important advantage. Similarly, the combination of digitization and networking can be employed to develop a common tactical picture that reduces the fog of war to clearly identify the positions of friendly forces and the known positions of the enemy. The ability to provide such a picture provides an example of developing an information advantage through NCW. Combat power can be increased sharply by successfully exploiting this advantage.

Across a broad spectrum of mission areas, evidence collected to date indicates that the development of a common operational picture (COP), such as that depicted in **figure 9**, can significantly increase the warfighter's awareness and understanding of tactical and operational situations. The sharing of information obviously contributes to shared situational awareness and understanding. The ability to develop a higher level of situational awareness, in less time than an adversary, combined with the ability to act on it, is a source of considerable warfighting advantage. This advantage is not intuitive, but its impact is profound.

Network-Centric Operations

"A networked Joint Force is able to maintain a more accurate presentation of the battlespace built on the ability to integrate intelligence, surveillance, and reconnaissance, information and total asset visibility. This integrated picture allows the JFC to better employ the right capabilities, at the right place and at the right time. Fully networked forces are better able to conduct distributed operations."

Department of Defense, Joint Operations Concepts, November 2003, p. 16.

Network-Centric Operations

NCO and the Joint Operations Concepts

Network-centric operations (NCO) involve the application of the tenets and principles of NCW to military operations across the spectrum of conflict from peace, to crisis, to war. The development of network-centric forces by the U.S. Armed Forces and the increasing readiness of commanders at all levels to apply the principles of NCW to the planning and execution of military operations are resulting in new capabilities of our joint, land, naval, air, space, and special operations forces.

Due in part to rapidly evolving concepts about how NCO will be conducted, perspectives are changing about how wars and other military operations will be conducted by the U.S. and our allies. As mentioned in the first chapter, NCW is central to the Department's force transformation efforts. The basic tenets and governing principles of NCW had a significant impact on the development of the *Joint Operations Concepts (JOpsC)* approved by the Secretary of Defense in November 2003.[24] They have also influenced the development and refinement of the subordinate Joint Operating Concepts (JOC), Joint Functional Concepts (JFC), and Joint Integrating Concepts (JIC).

"Networked" is one of the seven attributes, identified by the *JOpsC*, that the future Joint Force must possess, the others being "fully integrated," "expeditionary," "decentralized," "adaptable," "decision superiority," and "lethality." Networked, according to the *JOpsC*, "describes a Joint Force that is linked and synchronized in time and purpose. The Joint Force capitalizes on information and near simultaneous dissemination to turn information into actions. Networked joint forces will increase operational effectiveness by allowing dispersed forces to more efficiently communicate, share a common operating picture, and achieve the desired end-state. A networked Joint Force expands its reach. Reachback is the ability of the Joint Force to extend beyond organic capabilities to include fire support, sustainment, and information. This network includes interagency, designated multinational partners, academic and industrial sources, and includes both technical linkages and personal relationships developed through training and habitual association."[25]

As stated in the April 2003 *Transformation Planning Guidance (TPG)*, the key to the Department's transformation strategy is the development of future JOCs.[26] These concepts must be specific enough to permit identification and prioritization of transformation requirements inside the defense program, yet flexible enough to absorb valuable new ideas as they emerge. The overarching *JOpsC* provides the operational context for military transformation by linking strategic guidance with the integrated application of Joint Force capabilities.

JOCs are further developing key areas of the *JOpsC*. Focusing at the operational level and above, JOCs describe how a Joint Force Commander will plan, prepare, deploy, employ, and sustain a joint force given a specific operation or combination of operations. As shown in **figure 10**, four initial cornerstone JOCs have been developed: Homeland Security, Major Combat Operations, Stability Operations, and Strategic Deterrence.

Like the *JOpsC*, the JOCs are expected to evolve over time to reflect insights gained from experimentation and actual operations. All are based, at least in part, on the availability of networked forces and the implementation of the NCW theory by joint forces. The Service transformation roadmaps have identified the desired operational capabilities needed to implement the JOCs and the preferred means of obtaining those capabilities, including the essential capabilities for conducting NCO.

As an example of a JOC explicitly taking into account the availability of network-centric capabilities and the ongoing implementation of NCW theory, Version 1.10 of the *Major Combat Operations (MCO) JOC* identifies "seven core building blocks that form the foundation for U.S. success in future major combat operations." One of the seven is: "Use a coherent joint force that decides and acts based upon pervasive knowledge." This particular core building block involves the employment "of a network-centric method to collect, fuse, analyze, then provide access to information supporting leader decision requirements" and "a joint military/interagency decision making process that uses a collaborative information environment and functions with coalition partners … The network tools of the Information Age allow a degree of interdependence among Service forces that had always been desired but had never been achievable. Interdependence, to be sure, relies upon technical connectivity that maximizes machine-to-machine interface when and how that makes sense, but even more importantly it relies upon breaking down long-developed cultural positions and barriers."[27]

Joint Functional Concepts articulate how the future Joint Force Commander will integrate a set of related military tasks to attain capabilities required across the range of military operations. They are broad, but derive specific context from the JOCs. Existing JFCs include: Battlespace Awareness, Command and Control, Force Application, Focused Logistics, and Protection. Joint Integrating Concepts are intended to be building blocks for JOCs or JFCs and will describe how a commander integrates functional means to achieve operational ends. Existing JICs include Forcible Entry Operations and Undersea Superiority; JICs for Global Strike Operations, Sea-Basing Operations, Integrated Missile Defense, Joint Logistics, and Joint C2 are being developed.

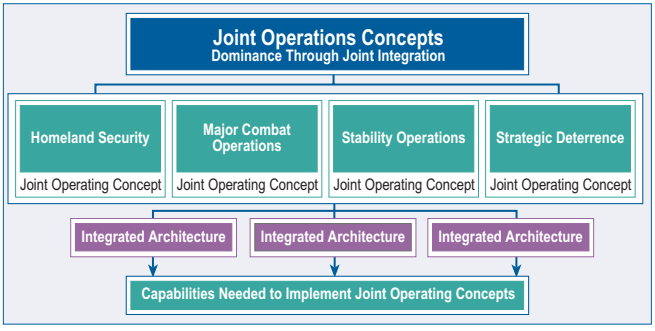


Figure 10: Joint Operations Concepts

NCO in Afghanistan and Iraq

"You are looking at the implementation of network-centric warfare, which is a growing implementation and will go on for a very long time. We are looking at a shift in sources of power. . . . when the lessons learned (from Operation Iraqi Freedom) come out, one of the things we are probably going to see is a new air-land dynamic. . . . we will have discovered a new 'sweet spot' in the relationship between land and air warfare, and a tighter integration between those. The things that compel that are good sensors, networked with good intelligence, disseminated through a robust network of systems which then increases speed."

Vice Admiral (Ret.) Arthur K. Cebrowski,
Director, Force Transformation
From remarks to the Defense Writers Group,
April 23, 2003.

The real-world experience of partially networked U.S. and coalition forces during recent combat operations in Afghanistan (Operation Enduring Freedom, 2001–2002) and Iraq (Operation Iraqi Freedom, 2003) has provided preliminary, yet powerful, evidence about the value of NCW and the conduct of NCO. More extensive studies and assessments are expected to follow.

Operation Enduring Freedom (2001–02): The network-centric capabilities of U.S. Central Command (USCENTCOM) elements during the conduct of Operation Enduring Freedom in Afghanistan proved vital to the defeat of Taliban and al Qaeda forces throughout the country. U.S. forces conducted operations in a mountainous, landlocked country the size of Texas that presented an extremely challenging environment. The long-sought goal of networking weapons platforms with sensor platforms came to fruition in this austere environment where both the need and the advantages were readily apparent.

USCENTCOM employed Special Operations Forces (SOF) teams on the ground working directly with our Afghan allies. These SOF elements were networked with other friendly forces on the ground and U.S. aircraft capable of delivering advanced precision-guided munitions. This combination proved extremely effective. Networking the sensors and the shooters in real time was only part of the requirement, however. Taliban and al Qaeda targets during Operation Enduring Freedom were often fleeting and weapons platforms had to be updated very quickly while in the air. In the case of B-2 bombers flying from bases in Missouri and B-1 bombers flying from other bases far from the theater of operations, this required a capability to change mission-tasking enroute to the target area in Afghanistan. Carrier-based aircraft needed a similar capability to deal with the dynamic nature of their targets.

Unmanned aerial vehicles (UAV) were used to a greater degree than ever before. The ability to pass information gathered by Predator and Global Hawk UAVs to ground commanders in Afghanistan enabled near-real-time battlefield situational awareness. The geographic location of the combatant command headquarters presented some

challenges for network-centric operations. Nevertheless, the USCENTCOM headquarters in Tampa was successfully networked with a forward headquarters in Kuwait and a subordinate forward headquarters in Uzbekistan. Satellite communications and related technologies enabled this networking capability to a degree not previously achievable.

Operation Iraqi Freedom (2003): The impressive network-centric capabilities of U.S. forces on display during OEF in Afghanistan were clearly evident during the conduct of Operation Iraqi Freedom (OIF). Many significant improvements in these capabilities were apparent by the time OIF began in March 2003. Network-centric capabilities provided, without question, a major contribution to the decisive victory of U.S. and coalition forces over Saddam Hussein's forces during major combat operations in Iraq during March and April 2003.

Network-centric capabilities evident in U.S. forces during OIF included not only the technology and systems that enabled the effective conduct of NCO, but innovative new concepts for the employment of the technology and an enhanced understanding of the human side of the NCW equation as well—highly trained, motivated Soldiers, Sailors, Airmen, and Marines fighting as part of an integrated, networked joint force. The implementation of NCW is, after all, about human behavior, not just new technology.

The effectiveness of NCO as conducted by U.S. and coalition forces during OIF has been strongly praised by senior commanders, including General (Ret.) Tommy Franks, Commander of the CENTCOM and coalition forces during OIF, and other commanders at all echelons of command down to battalion and company level.[28]

Most of the groundwork for the information network and other network-centric capabilities that empowered our forces during OIF was actually completed during OEF. After the success of U.S. forces in Afghanistan in 2001–02, the gradual buildup to the war in Iraq allowed careful planning and positioning to provide the necessary technologies and systems that enabled commanders to conduct high speed, non-contiguous NCO and, when necessary, to change plans as rapidly as the situation required. According to Brigadier General Dennis Moran, then CENTCOM/J-6, "The rapid sharing of information at all levels of command was possible because of the technology we had in place. The ability to move intelligence rapidly from the sensor to either an analytical decision maker or directly to the shooter was the best that we have ever seen … We validated the concept of network-centric warfare and the need for communications, C2, and ISR systems to be hooked up to, and interoperable with, the Global Information Grid and to be adaptable to whatever circumstances are on the battlefield."

One of the biggest challenges during OIF, according to General Moran, involved sharing information with coalition partners. "Our ability to take information drawn predominantly from systems on the U.S.-only network, and then being able to rapidly, seamlessly move those into a coalition network, was extremely challenging. We had some workarounds that were less than fulfilling, but one of the biggest challenges we faced was sharing timely information in a seamless manner with our coalition partners. That's one of the key take-aways of this conflict."[29]

The Director, OFT, in referring to the emerging NCW capabilities that gave U.S. and coalition forces a warfighting advantage during OEF and OIF, observed that, "DoD (now) has experience in network-centric warfare … people have put their hands on it, they have seen it in action. They realize that in western Iraq you couldn't possibly have done the non-contiguous battlespace operation without being very well networked. The Department is, in fact, internalizing these lessons and making the appropriate adjustments."[30]

Among the lessons learned from OIF is a realization of how NCW works operationally and the impacts this realization may have on materiel and force organization. The Office of the Secretary of Defense, JFCOM, the Services, and other DoD organizations are likely to study networked capabilities and their role during OIF "not as a template for future action but as a model of some capabilities that may be desirable to implement in the future."[31]

NCO Conceptual Framework

The Office of Force Transformation (OFT) and the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD [NII]) have collaborated for several years on an effort to develop metrics to test the working hypothesis and tenets of NCW. The primary objective has been to develop a rich and comprehensive set of NCW-related metrics that could be used in experimentation and other research endeavors to gather and evaluate evidence concerning NCW and NCO. Potentially, this evidence could then be used to inform DoD investment decisions across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) functional areas. Thus far, the results of this effort have included the development of the NCO Conceptual Framework (CF), the conduct of related case studies, and a variety of other NCO-related research, outreach efforts, and publications.[32]

The NCO CF identifies key concepts and linkages to output measures in the NCO value chain in the context of the four domains of Information Age warfare: physical, information, cognitive, and social. The NCO CF is intended to help guide and measure NCW implementation in the Department of Defense through its application to various mission sets or scenarios. The CF has been designed to help answer the "why" question. One of its main purposes is providing the means to explain the dramatic increases in effectiveness that are evident when network-centric capabilities are acquired and network-centric practices are adopted by military forces.

Version 1.0 of the NCO CF was published in November 2003; Version 2.0 (Draft) followed in June 2004. An international team of government,

industry, and academic personnel organized by OFT and OASD (NII) continues to evaluate and refine the NCO CF and conduct a series of NCO case studies. **Figure 11** shows the current version of the top-level NCO CF.[33] An earlier version of the CF was successfully applied and initially validated using an air-to-air case study. In order to refine and validate the NCO CF, it is being applied to a broad range of mission areas in both combat and peacetime training environments.

Seven case studies of the CF have been completed, all involving its application to various mission areas:

- Air-to-air operations;
- Ground maneuver operations (Stryker Brigade Combat Team);
- US/UK coalition operations during Operation Iraqi Freedom (OIF);
- Air-to-ground operations (close air support);
- Special operations (Naval Special Warfare Group One);
- Multinational operations (NATO); and
- Naval operations (Commander Task Force Fifty) during Operation Enduring Freedom (OEF).

Additional case studies are currently in the planning or early initiation stages including: ground maneuver operations (V Corps and 3rd Infantry Division) during OIF; stability and restoration operations; and crisis management operations. Version 2.0 of the NCO CF will be finalized, using feedback from the case studies.

OFT's effort, in partnership with OASD (NII), to develop and refine the NCO CF is aimed at supporting two of the Director, OFT's "Top Five Goals":

- Implement NCW as an emerging theory of war for the Information Age and the organizing principle for national military planning and joint concepts, capabilities, and systems.
- Get the decision rules and metrics right and cause them to be applied enterprise wide.

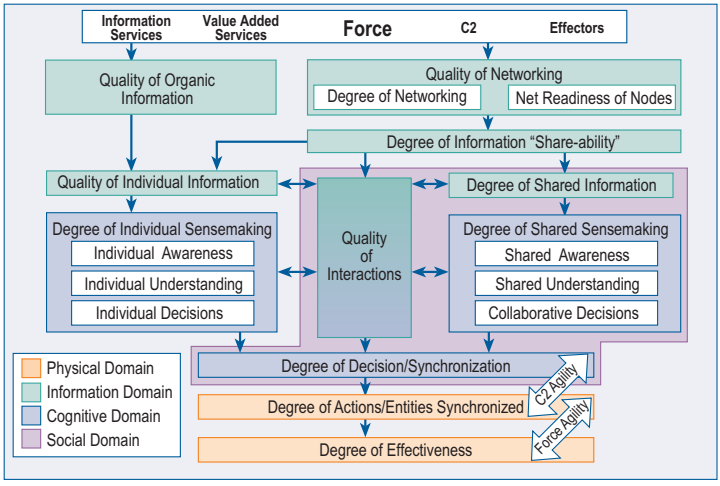


Figure 11: Top-Level NCO Conceptual Framework, Version 1.0

Specific near-term objectives associated with the development of the NCO CF are:

- Develop and codify the underlying theory of network-centric warfare through development and refinement of an underlying conceptual framework for analysis and assessment;
- Apply the conceptual framework to a range of mission areas and assess its ability to explain key underlying relationships between input variables and output measures;
- Support the application of the conceptual framework to help facilitate requirements definition for network-centric concepts, capabilities, and systems (e.g., FORCEnet, C2 Constellation, Future Combat System);
- Develop analytic methodologies that can be applied to enhance the planning and execution of experiments that explore and validate network-centric concepts as well as the training and evaluation of networked forces; and
- Develop an enhanced understanding of the challenges associated with allied and coalition network-centric operations.

NCO Case Studies

The NCO Conceptual Framework initiative is enhancing our understanding of NCW and NCO by gathering and analyzing evidence on NCO-related technologies and practices. The seven completed NCO case studies have provided the primary vehicle for applying the NCO CF, gathering the data, and analyzing the evidence. The following summaries of four case studies illustrate the progress to date.

Ground Operations (Stryker Brigade Combat Team): The results of the Stryker Brigade Combat Team (SBCT) NCO Case Study demonstrate the power of NCW capabilities. The Army's SBCT is a new force design utilizing an information-centric concept of operations; enhanced vehicle speed and stealth based on the Stryker wheeled fighting vehicle; improved reconnaissance, surveillance, and target acquisition (RSTA) capabilities; and first-generation NCO capabilities including interim mobile networks, satellite communications, and evolving battle command systems.

The hypothesis explored by this case study was that the NCO capabilities of the SBCT would enable information and decision superiority and increase force effectiveness. The study objective was to understand how the Stryker Brigade's NCO capabilities could actually provide these advantages and if they could provide additional combat power.

The operational environment for the Stryker Brigade case study was a small-scale contingency involving early entry operations in a rapid response and deployment scenario. The data collection and analysis were focused on a Stryker Brigade Joint Readiness Training Center (JRTC) exercise conducted in May 2003. The baseline for comparison

was a non-digitized light infantry brigade, the SBCT's "closest predecessor." The quality of situational awareness, situational understanding, speed of command, quality of decisions, and force self-synchronization were used in the case study as measures of command and control (C2) effectiveness. Similarly, force effectiveness and survivability were used as measures of mission effectiveness (MOEs).[34]

The results of the SBCT Case Study demonstrated that the Stryker Brigade is significantly more agile and capable than a non-digitized light infantry brigade. Based on the analysis, the following observations concerning the Stryker Brigade's NCO capabilities have been made:

- Several key NCW factors contribute to an order-of-magnitude increase in Stryker Brigade force effectiveness:
  - –75% of SBCT with networked battle command systems;
  - –Selected high bandwidth beyond line-of-sight satellite communications links;
  - –Increase in individual/shared information quality from 10% to 80%;
  - –Acceleration of speed of command from 24 to three hours in key engagements; and
  - –Ability to control speed of command.
- Key result from SBCT certification exercise at JRTC—friendly vs. enemy casualty ratio decreased from 10:1 to 1:1.
- Caveats:
  - –Stryker's mobility—soldiers arrived fresh for battle;
  - –Other factors contribute to increase in force effectiveness—training, leader development, personnel stabilization, and firepower; and
  - –Current results may underestimate future potential of SBCT's NCW capabilities in land warfare.

In conclusion, significant NCW capabilities were effectively demonstrated by the Stryker Brigade mission capability package (MCP). The Brigade's new organizational structure, battle command and networking capabilities, and evolving operational concepts improved the quality of information available to soldiers throughout the unit. In turn, improved information quality resulted in improved interactions and collaboration, which led to enhanced shared awareness and understanding. Ultimately, the Brigade's NCW capabilities provided commanders with better decision options and enabled better control of the speed of command. Collectively, all of these information-based attributes made the Stryker Brigade's decision-making ability more agile. These qualities, along with improved organizational, equipment, and training capabilities, increased combat effectiveness.

US/UK Coalition Operations During Operation Iraqi Freedom: This case study examined United States/United Kingdom coalition land combat operations during OIF (February–April 2003). The focus was on the use of NCO technologies and practices, specifically the use of the Force XXI Battle Command Brigade and Below (FBCB2)/Blue Force Tracker (BFT) system by ground forces. FBCB2/BFT is a digital network that allows users to send and receive information across the battlefield. It consists of a computer equipped with communication and global positioning system (GPS) transceivers and is designed to work with brigade-and-below operators. It not only displays the location of blue force elements, but also mapping and satellite imagery. BFT is also capable of creating graphical overlays, assisting in the conduct of terrain analysis, and providing text messaging.

The objective of this case study was to assess the effectiveness of a networked force (relative to a non-networked force) in high-intensity combat, utilizing the NCO CF as the vehicle for research. The study sought to identify levels of effectiveness related to the degree of networking. The hypothesis examined in the study was that during Operation Iraqi Freedom, as compared to previous operations and training without NCO capabilities, the direct accessibility to NCO capabilities by U.S. and UK units improved individual sensemaking, enhanced the quality of interactions, improved shared sensemaking, and increased mission effectiveness.

The initial focus of the case study was on land combat operations conducted by the UK's 1st Armored Division. Subsequently, land combat operations of the 1st Brigade Combat Team (1BCT) of the U.S. Army's 3rd Infantry Division (3ID) were also analyzed. Three key factors contributed to the degree to which FBCB2/BFT was successfully employed and exploited by coalition forces: density of deployment, scheme of maneuver, and degree of training.

The density of deployment varied between U.S. and UK forces. The 3ID deployed approximately 150 units, which enabled deployment down to the company level. The UK 1st Armored Division deployed 47 units, which translated to a significantly reduced deployment footprint. The scheme of maneuver for the U.S. and UK forces also varied significantly. The vast distances that the 3ID operated over in advancing from Kuwait to Baghdad significantly stressed line-of-sight terrestrial communications capabilities and placed a premium on the SATCOM-enabled digital communications. In contrast, the UK 1st Armored Division's scheme of maneuver was geographically less dispersed and its three major subordinate units (3rd Marine Commando Brigade, 7th Armored Brigade, 16th Air Assault Brigade) were able to use their terrestrial and SATCOM voice communications to develop situational awareness and perform command and control. In key instances, FBCB2/BFT contributed to the development of enhanced situational awareness within the UK forces. The degree of training with the new equipment also varied between U.S. and UK forces, but both found the system valuable during OIF.[35]

The employment of FBCB2/BFT by U.S. forces (3ID's 1BCT) during OIF had a dramatic effect on the speed of command and effectiveness:

- FBCB2/BFT provided tactical commanders with enhanced situational awareness relative to previous operations and exercises when the system was not available.
- The FBCB2/BFT system was primarily used to augment situational awareness provided from other systems.
- FBCB2/BFT was used as a tool for mission planning and the conduct of operations.
- The FBCB2/BFT system improved "macro" situational awareness.
- FBCB2/BFT provided a facilitating capability for coalition operations.

The limited deployment, training, usage, and operation of FBCB2/BFT with UK units limited the contribution to overall situational awareness. Evaluation of the UK forces' use of BFT revealed the following:

- Although the FBCB2/BFT was not used widely, it was perceived as providing a good, if limited, situational awareness picture.
- The currency, precision, and consistency of information provided by FBCB2/BFT were rated significantly higher than the baseline.
- Uncertainty in shared sensemaking using FBCB2/BFT is much higher, largely because of limited combat net radio interactions between units and delays/errors in passing information up and down the chain of command.
- Many UK participants agreed there was great potential for utilizing FBCB2/BFT to communicate boundaries, command intent, and reports, but none had done so during OIF.

Several lessons from the employment of FBCB2/BFT during OIF were common to U.S. and UK forces:

- FBCB2/BFT does not replace voice communications in ground combat operations—it augments it.
- A ground combat unit's effectiveness also depends on its combat support (CS) and combat service support (CSS) assets; like the ground combat units they support, CS and CSS units also require high-quality situational awareness. Thus, the FBCB2/BFT system should be integrated with CS and CSS elements.

Air-to-Ground Operations: This case study focused on air-to-ground engagements, and specifically examined the role of NCO technologies and practices in support of close air support (CAS) operations. The central focus of the study was to answer three questions. First, what explained the successful results of certain nighttime CAS missions during the U.S. Army's Division Capstone Exercise—Phase 1 (DCX-1) at the National Training Center in 2001? Second, to what extent were NCO technologies and practices, such as those used in DCX-1, employed during Operations Enduring Freedom (2001–2002) and Iraqi Freedom (2003)? Third, what was the impact of their use on mission effectiveness?

In analyzing the results of DCX-1, the study concluded that two factors directly contributed to the dramatic success realized by CAS: The robust networking of both ground and air forces; and the employment of precision engagement capabilities by the CAS aircraft.

The evidence showed that the robust networking enabled an order-of-magnitude improvement in information sharing across the air-ground seam, which in turn enabled CAS pilots to develop a common tactical picture of the Blue and Red ground forces. This common picture in turn enabled the CAS pilots to develop very high levels of shared awareness, which, when combined with their precision engagement capabilities, enabled them to decisively engage the opposing force (OPFOR) in close proximity to Blue ground forces. The net result was that the training exercise had to be stopped and restarted to enable the Blue force to engage the OPFOR and achieve their training objectives.

The study next examined CAS operations during OEF and concluded that SADL use between air and ground elements was limited due to ground unit equipment constraints. However, SADL was effective in coordination among aircraft in support of ground operations, and Litening Pods were effective in air-ground coordination. Preliminary findings during OEF indicated that there was little air-ground networking at the tactical level.

Finally, the air-to-ground operations case study examined CAS in OIF and determined that NCO technologies and practices provided U.S. forces in Iraq with the ability to reconcile air and ground perspectives and successfully attack ground targets in a limited number of engagements. Most CAS missions conducted during OIF depended primarily on legacy systems at the aviator-ground maneuver element level. Both Army and Marine ground units usually called for CAS and guided CAS aircraft to the target using voice communications. However, NCO systems were used extensively between air and ground components at the operational level and within component chains at all levels. Multiple network-centric systems supported networking between staffs.

Overall, the results of this case study show that there is room for much improvement in networking CAS operations at the tactical level. In recognition of this problem, the Services "are pursuing equipment, concepts, and experiments that leverage NCO at the tactical level." On the other hand, "the use of relatively robust NCW systems" at the operational level provides a "a measurable improvement in the confidence and trust of the warfighters and ultimately, improved combat effectiveness." When available to pilots and ground troops at the tactical level, network-centric systems will further enhance CAS engagements, reducing the kill-chain timeline and contributing to improved responsiveness and flexibility. Already, these NCW systems are allowing air controllers at higher levels of command to gain enhanced situational awareness; this, in turn, is beginning to change the traditional definitions of "tactical" and "operational."[36]

Special Operations (Naval Special Warfare Group 1): This case study focused on the role of NCO in the activities of the Naval Special Warfare Task Group 1 (NSWG-1), a U.S. Navy special operations forces (SOF) unit, during OEF and OIF. The manner in which NSWG-1 conducted its missions during OEF and OIF demonstrated its ability to exploit NCO technologies, organizational structures, and processes during combat operations. Across all mission types, the Navy SEAL teams of NSWG-1 overcame harsh operating conditions and were able to dramatically improve the mission planning process, resulting in improved force effectiveness. They did so by developing and utilizing network-centric capabilities. NSWG-1's unprecedented success during OEF and OIF illustrated the tenets of NCO: better quality networking leads to enhanced information sharing, improved collaboration, and increased speed of command and self-synchronization.

The purpose of the case study was to document and explain the exceptional performance of NSWG-1 during OEF and especially OIF. It focused on NCO technologies and practices—the people, processes, and technologies used in the conduct of war planning and fighting. The basic hypothesis explored was that the innovative co-evolution of NSWG-1's Mission Support Center (MSC), along with the development, adoption, and adaptation of new information technologies, improved mission planning and execution.

The capabilities facilitated by NSWG-1's MSC clearly provided additional support to the forward elements of NSWG-1, both the warfighters and support staff. The MSC enabled enhanced collaboration among and between forward and rear SEAL units. This collaboration was made possible by a dramatically improved physical networking infrastructure and information management system. Ultimately, the MSC was responsible for shared situational awareness that enabled SEAL planners and warfighters to plan and execute successful missions.

The results of this case study indicate that measurable improvements in speed of decision making and synchronization at the unit and team level were achieved with the evolution of the NSWG-1 mission capabilities between the beginning of OEF and the end of OIF. The improvements evident during OIF were achieved as a result of more leveraging of reachback support at the MSC. Measurable improvements in NSWG-1's network-centric capabilities resulted in enhancements in information sharing, collaboration, and the decision-making process. Additionally, SEAL teams gained an enhanced ability to conduct distributed, collaborative planning and were able to sustain a higher operational tempo during OIF compared to OEF.[37]

NSWG-1 assessed the improvements achieved between the beginning of OEF and the end of OIF. They concluded that these improvements significantly increased NSWG-1's combat power by increasing the number of combat missions that could be simultaneously conducted worldwide. Other highlights of their findings included:

- Enhanced Command and Control (NSWG-1):
  - –Increased mobility of the commander and his key battle staff;
  - –Effective information management provided commander with rapid, tailored, decision-quality information;
  - –Increased global situational awareness for the operational commander;
  - –Increased consistency of global planning efforts; and
  - –Increased survivability—reduced force protection concerns.
- Increased mission effectiveness (Naval Special Warfare Task Unit [NSWTU]):
  - –Increased quality of information;
  - –Increased situational awareness at the unit level;
  - –Increased time available for mission planning and rehearsal; and
  - –Reduced risk—increased probability of mission success.

NCW Implementation

"Transformation is yielding new sources of power … One such source is information sharing through robust network structures. We have a mountain of evidence—from simulation, from experimentation, and from real world experience—that substantiate the power of network behavior … Each of the Departments' efforts reflects an understanding of this phenomenon … These efforts reflect the ongoing shift from platform-centric to network-centric thinking that is key to transformation."

Vice Admiral (Ret.) Arthur K. Cebrowski,
Director, Force Transformation, Office of the Secretary of Defense,
Prepared Statement for the Senate Armed Services Committee,
March 14, 2003.

NCW Implementation

Transformation, including the implementation of NCW capabilities to enable the joint force and the ongoing shift from platform-centric to network-centric thinking, is a continuing process with no discernible end point. Those involved in transformation and NCW implementation in the Department of Defense (DoD) must anticipate the future and wherever possible help create it. Transformation and NCW implementation deal with the co-evolution of the seven key functional areas of doctrine, organization, training, materiel (technology), leadership and education, personnel, and facilities (DOTMLPF) **(figure 12)**. Consequently, progress in implementing network-centric warfare cannot be measured solely by focusing on one dimension, such as technology or doctrine. Rather, progress must be assessed in terms of the maturity of mission capabilities that integrate key elements of DOTMLPF.

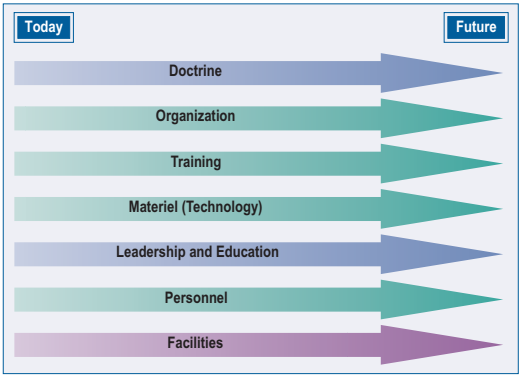


Figure 12: NCW Implementation—Co-Evolution of DOTMLPF Functional Areas

A profound change in any one of these areas necessitates changes in all. Ultimately, military transformation and NCW implementation are about changing the values, attitudes, and beliefs of the U.S. Armed Forces concerning how combat power is developed and employed.

At the Joint and Service levels, significant progress is being made in developing NCW capabilities that leverage the power of order-of-magnitude improvements in information sharing enabled by networking. The NCW-related initiatives described in the first two sections of this chapter, "Joint NCW Implementation" and "Service NCW Implementation," provide a snapshot of the myriad of activities that are being pursued across DoD to help enable NCW. Therefore, the discussion of U.S. NCW-related initiatives that follows is not meant to be exhaustive, but rather representative.

To varying degrees, the U.S. Joint and Service initiatives described in this chapter are enabling the components of the NCW value chain described previously in this document by improving our forces' capabilities to:

- Improve information sharing;
- Enhance the quality of information;
- Increase shared situational awareness;
- Enhance collaboration;
- Enable self-synchronization;
- Enhance sustainability;
- Increase speed of command; and
- Improve mission effectiveness.

The third and final section of this chapter, "Allies and Multinational Partners," offers a brief look at the impressive efforts of U.S. allies and multinational partners to develop or enhance their network-centric capabilities. These international developments, including the ongoing efforts of NATO to study a NATO Networked Enabled Capability (NNEC) and develop an overarching Strategic Framework and Concept for NNEC, are very promising for the conduct of combined network-centric operations (NCO) in the future.

Joint NCW Implementation

A number of new operational concepts, organizations, and systems are being developed to enable a networked Joint Force. Impressive new network-centric capabilities such as the Force XXI Battle Command Brigade and Below (FBCB2/BFT)/Blue Force Tracking (BFT) system, so valuable to Army, Marine Corps, and Special Operations units during Operation Iraqi Freedom (OIF), are providing significant enhancements in shared situational awareness and other vital areas of NCW. FBCB2/BFT and the other initiatives described in this section are enabling U.S. forces to conduct increasingly effective network-centric operations (NCO) across the full range of military operations. In addition, significant efforts are underway within the Department to promote cultural change in the U.S. military through training and education.

FBCB2—Blue Force Tracking: Joint network-centric capabilities gave U.S. forces unprecedented advantages during the conduct of OIF in March–April 2003. A prime example was the Army's satellite-based FBCB2 system, also referred to as the Blue Force Tracker, successfully employed by Army, Marine Corps, Special Operations Forces, and British ground forces (1st UK Armored Division) during OIF. The system uses Global Positioning System (GPS) transmitters mounted in military vehicles and aircraft to monitor their locations. The information is combined with terrain maps and intelligence on enemy positions to create a battlefield picture that can be shared over commercial satellite networks **(figure 13)**.

Figure 13: FBCB2—Blue Force Tracking

General Tommy Franks, USA (Ret.), commander of U.S. Central Command and the coalition forces during OIF, credited network-centric warfare, and the Blue Force Tracker in particular, with enabling the Army and Marine Corps' ability to work together and track each other's progress throughout the operation. It was by all accounts a major factor in reducing incidents of friendly fire during OIF. According to General Franks, FBCB2 gave ground commanders a "precise sense of the location, capacity, and capability of the

battlefield. What a powerful, powerful thing!" He added that he personally used the Blue Force Tracker to watch in "near-real-time" as leading elements of the Army's 3rd Infantry Division approached and entered Baghdad in early April.[38]

While FBCB2's performance during OIF has been widely praised, the Army is looking for ways to better collect data across the forces and feed it into the system. In the words of Colonel Nick Justice, USA, FBCB2 Program Manager prior to and during OIF, "What we need is common, shared information that I might use in different ways to meet everyone's needs, whether they're a logistician, a combat company commander, or a theater-level Army commander."[39]

Horizontal Fusion—a Catalyst for Net-Centric Transformation: The Horizontal Fusion Portfolio of the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) is one of DoD's most comprehensive and promising efforts for advancing the implementation of net-centric[40] capabilities in the U.S. Armed Forces. It was created in early 2003 to respond to Secretary of Defense Rumsfeld's vision of force transformation and to achieve "power to the edge" in the new battlespace. Horizontal Fusion equips warfighters, or "Edge-Users," with the ability to access the information they need at the right time to make the right decisions. The initiative has integrated and demonstrated net-centric capabilities that will transition directly into operational capabilities.

Horizontal Fusion is the catalyst for the net-centric transformation of the DoD. It will provide real-time situational awareness throughout the battlespace, sensemaking tools, multi-community-of-interest collaboration, and critical intelligence information sharing. The Horizontal Fusion Portfolio integrates advanced technologies to make the "Quantum Leap" to NCO, with an emphasis on support to the warfighter. Horizontal Fusion is one of the pillars of the Department's NCW/NCO transformation effort, which includes Global Information Grid Bandwidth Expansion (GIG-BE), Joint Tactical Radio System (JTRS), Wideband Satellite Communications (SATCOM), Net-Centric Enterprise Services (NCES), and Information Assurance (IA).

The term "horizontal" refers to the ability to reach across traditionally stove-piped organizations; and "fusion" refers to the process and applications that allow net-centric "melding." Users will be able to seek the information they need across the battlespace through "smart-pull" and, in turn, information sharing. This process is described by the verbs task, post, process, and use (TPPU). With TPPU, the user can smart-pull information in seconds rather than minutes. To be effective, the TPPU process requires interoperable infrastructures within the DoD and across external U.S. and coalition intelligence-gathering organizations. Real-time collaboration allows users, regardless of their respective communities of interest, to share insights and add value to posted information; it will also allow geographically separated commanders and units to act as a cohesive team by sharing a common operational picture (COP).

The aim of Horizontal Fusion is to establish standards, policies, and procedures for future Web-enabled capabilities. This represents a significant change in culture for security, acquisition, and fielding. As currently envisioned by the ASD (NII), the Horizontal Fusion initiative will "end" in 2008, leaving a new acquisition mindset among the Services and Defense Agencies. Horizontal Fusion has annual goals that touch all areas in net-centricity. Each year's portfolio of initiatives expands on the capabilities and standards of the previous year. Ongoing and new capabilities that are ready to be fielded are demonstrated through the annual Quantum Leap demonstration, a proof-of-concept demonstration of the operational Horizontal Fusion capabilities at multiple geographical locations. It is the graduation of the year's capabilities to operations.

The 2003 Horizontal Fusion objectives included the following: searching capabilities through edge computing power; providing users with the ability to publish to the GIG; sharing intelligence, surveillance, and reconnaisance (ISR) data; improving operations within DoD and the intelligence community; and exploiting diverse data sources. The 2004 Portfolio expands the collateral space to more communities of interest by integrating operational NCES with organizations and programs that hone capabilities and services that can be readily adapted to the collateral space. Horizontal Fusion is working cross-domain and secure wireless security issues using architectures designed by the National Security Agency (NSA) and other intelligence and security organizations. The Horizontal Fusion Portfolio membership includes DoD, industry, and multinational partner programs. The sponsors of current initiatives now in the Portfolio include the Army, Navy, and Air Force; U.S. Pacific Command; U.S. Strategic Command; Defense Intelligence Agency; National Geospatial-Intelligence Agency; National Security Agency; Department of State; North Atlantic Treaty Organization; and several DoD industry and education programs.

Sense and Respond Logistics: An initiative sponsored by the Office of Force Transformation (OFT), Sense and Respond Logistics (SRL) is an emerging logistics concept tied closely to NCW theory and practice, as evidenced by some of its main characteristics: shared awareness, speed and coordination, dynamic synchronization, adaptability and flexibility, and networked organization. In general, SRL is an adaptive method for

maintaining the operational availability of units by managing their end-to-end support network. Units operating under the SRL concept are networked and dynamically synchronized to satisfy demand in response to changes in the environment. Therefore, all units within that network are potential consumers and providers of supply to and from all other units in the network.

The development of SRL involves not only the implementation of a new concept, but also the infusion of key technologies, the realignment of the logistics infrastructure, and the inclusion of new processes that fully exploit the concept. **Figure 14** highlights three approaches to logistics—Mass-Based, Just-in-Time, and Sense and Respond—and the ongoing transformation of the logistics function in military operations. As the SRL concept evolves, it is intended to parallel the changes underway in Joint Force operations. It relies on IT-enhanced adaptation and learning; translating to a distributed, adaptive systems capability; and resulting in rapid planning, coherent execution, and sustainment of military operations in complex, uncertain environments.

The SRL initiative has three goals. First, increase the robustness of logistics support to include the ability of sense and respond (S&R) networks to operate in an environment where communications and node connectivity may be restricted and security is challenged. Second, provide more flexibility to the commander; this flexibility is required by the more dynamic future battlespace. And third, increase the adaptiveness of the logistics system in order to decrease the reaction time required responding to environmental changes or new operational missions. In its ongoing efforts to help DoD achieve these goals, the OFT is sponsoring several projects and initiatives to move SRL from the concept phase to a new capability for the warfighter.

Figure 14: Transforming Logistics

Cultural Change and Education:

As mentioned at the outset of this chapter, military transformation and NCW implementation require changing the culture of the U.S. Armed Forces. Much of this vital cultural change can be accomplished by the implementation of educational reforms that will influence the attitudes, values, and beliefs of future U.S. military leaders and instill in them a sense of urgency to transform and to be innovators. The education of our future leaders will be crucial to the success of NCW implementation and the overall force transformation process in the DoD.

Accordingly, one of the highest priority objectives of the Office of Force Transformation since its establishment in late 2001 has been to act as a catalyst for cultural change within the Department. OFT's core initiative for facilitating cultural change is "Education for Transformation." This initiative is focused on developing and diffusing knowledge in areas that are key to transformation.

Other Joint NCW Initiatives:

- **Common Relevant Operational Picture for Joint Forces:** The Common Relevant Operational Picture (CROP) will present timely, fused, accurate, and relevant information that can be tailored to meet the requirements of the Joint Force Commander and the Joint Force. As the lead agent for this program and the systems engineer for the Joint Forces Command (JFCOM) in coordinating joint battle management C2 programs, the Air Force is working to achieve the CROP for joint forces through the Family of Interoperable Operational Pictures (FIOP) program. The FIOP is a multi-Service program with new funding provided by OSD that will close the seams between existing legacy C4ISR systems and extend the capability of systems under development in order to exploit the full data collection and management abilities of current C4ISR assets. In order to provide an all-source picture of the battlespace containing actionable, decision-quality information to the warfighter through a fusion of existing databases, this program will implement data-sharing and fusion among heterogeneous, stove-piped systems in support of users at the operational and tactical levels. It will facilitate the establishment of interoperability standards and architectures to guide future acquisitions.[41]

- **Standing Joint Force Headquarters (SJFHQ):** DoD is strengthening joint operations through the establishment of Standing Joint Force Headquarters (SJFHQ) at the Combatant Commands (COCOM). When fielded, each SJFHQ will provide a standing body of planners, who possess the full range of skills and training necessary to plan and conduct effects-based, joint operations, while employing the tenets of NCW. With an initial capability to be fielded at each of the COCOMs in FY05, the SJFHQ will provide the manning, equipment, training, and procedural enhancements needed to become a core around which the staff of a regional COCOM or a JTF commander can operate across the spectrum of operations from daily routine, through pre-crisis, to crisis response. The Deployable Joint C2 (DJC2) system will provide the material component of the SJFHQ.[42]

- **Collaborative Information Environment (CIE):** The CIE is the aggregation of hardware, software, and procedures that leverages the Global Information Grid (GIG) to enable sharing of information and collaboration within and among staffs, including interfaces with both DoD and commercial communications pathways. USJFCOM will provide an interim CIE toolset in conjunction with the initial fielding of the SJFHQ in FY05[43] In general, the CIE concept aims to provide common situational awareness and understanding to all decision makers by collaboratively linking the JTF staff and its components with the COCOM, interagency participants, and allied or coalition organizations.

- **Distributed Common Ground/Surface System:** DCGS is the Department's intelligence, surveillance, and reconnaissance (ISR) network-centric enterprise that provides Task-Post-Process-Use (TPPU) capabilities for the JTF and below. It is the key component for providing fused ISR-based decision-quality information for effective joint C2.[44]

- **Dynamic Joint ISR Concept:** The Dynamic JISR Concept applies a net-centric approach to the management of ISR capabilities to integrate sensors and processing capabilities into a coherent whole and thus better support the knowledge demands of the Joint Force Commander and his staff, his components, and multinational coalition forces. This concept supports and relies on collaborative planning and execution across the full range of military operations among international agencies, the intelligence community, and the Joint Force Commander and his Service components.[45]

- **Joint Interagency Coordination Group (JIACG):** The JIACG will establish operational connections between civilian and military departments and agencies to improve planning and coordination within the government. The JIACG will be a multi-functional, advisory element providing perspective on civilian agency capabilities, approaches, and limitations in the development of a coordinated use of national power. This will ensure the best mix of capabilities is employed to achieve the desired effects that include the full range of diplomatic, information, and economic activities. The potential requirements for achieving a fully networked JIACG during future contingencies are formidable.

Service NCW Implementation

For some time, the Services have recognized the tremendous leverage available to their personnel, organizations, and platforms/systems from the exploitation of NCW as an emerging theory of war and the increasing implementation of joint and Service NCW capabilities, not only for warfighting, but also across all mission areas and throughout the battlespace. Their progress and future plans in

this regard were evident in the first editions of the Service Transformation Roadmaps, published in 2002, and are even more apparent in the annual Roadmap updates of 2003 and 2004.[46] Whereas the authors of the 2002 Roadmaps were able to incorporate some of the NCW lessons learned from Operation Enduring Freedom in Afghanistan, the 2003 and 2004 Roadmaps have benefited from the additional combat experience gained by U.S. forces during Operation Iraqi Freedom, the occupation of Iraq in the face of multiple threats, continuing U.S. military operations in Afghanistan, and the completion of the Joint Operating Concepts (JOC).

The Services are accelerating their efforts to network their forces, develop innovative new concepts of operations tied to NCW in support of the JOpsC and the JOCs, experiment with new concepts and technology, enhance the readiness of their personnel and organizations to participate in joint networked operations, and, in general, to capitalize on the power of NCW theory and network behavior. The material in this section is drawn almost entirely from the *2003 Army Transformation Roadmap*, the *Naval Transformation Roadmap 2003*, and the *Air Force Transformation Flight Plan* (November 2003).

Army

"Transforming our Nation's military capabilities while at war requires a careful balance between sustaining and enhancing the capabilities of current forces to fight wars and win the peace while investing in the capabilities of future forces. Joint concept development and experimentation, science and technology (S&T) investment, and future force design that enables interdependent network-centric warfare will ensure future capabilities meet the requirements of tomorrow's Joint Force."

R. L. Brownlee, Acting Secretary of the Army
General Peter J. Schoomaker, USA, Chief of Staff
Foreword, 2003 Army Transformation Roadmap,
1 November 2003.

The Army, in coordination with the other Services, is developing transformational capabilities from an inherently joint perspective. In the near term, the Army will maintain and improve capabilities to enable the Current Force to conduct joint operations. At the same time, it will develop transformational capabilities for the Future Force.[47] Although the Future Force will be a hybrid force, one of the key future elements of the hybrid mix will be the Future Combat Systems-equipped Unit of Action. The FCS-equipped Unit of Action encompasses more than a new set of capabilities; rather, it reflects a fundamentally transformed method of combat.[48]

Enabling Interdependent NCW: The *Joint Operations Concepts (JOpsC)* identifies seven Joint Force attributes that the future Joint Force must embody to achieve "full-spectrum dominance." The *2003 Army Transformation Roadmap* (2003 ATR) describes how the Army is increasing its capabilities to achieve these attributes and is implementing the *JOpsC* and the JOCs.

As mentioned previously, "Networked" is one of the seven Joint Force attributes identified in the JOpsC.[49] In discussing its plans for networking its force and enabling interdependent NCW during the conduct of joint operations, the Army *Roadmap* states: "Information superiority and situational understanding are critical enablers for future joint operations. Operating in the collaborative information environment, Army forces will harness the power of the ongoing revolution in information technology to aid in the fusion of data and information to develop actionable and predictive intelligence and to link people and systems—horizontally and vertically—within the joint network to increase situational understanding. Army battle command capabilities will enable interdependent network-centric warfare within joint, interagency, and multinational full-spectrum operations."[50]

The Army is planning to accelerate the Future Force network to enhance the joint battle command capabilities of the Current Force. Building on recent efforts to analyze the development of current network architecture and supporting systems, the Army is reprioritizing development of the network to focus on top-down fielding to the Current Force. It is also leveraging experiences and lessons learned from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) to enhance joint battle command, including battle command on-the-move (BCOTM) and Blue Force Tracking (BFT) capabilities for select Current Force units. To ensure operating forces have the most advanced network capabilities, the Army is synchronizing the fielding of battle command capabilities with unit rotation schedules. Also, the Army continues to partner with Defense Agencies, other Services, the Joint Staff, and Joint Forces Command (JFCOM) in all aspects of network development.[51]

Future Combat System (FCS): The FCS is the Army's "multifunctional, multimission, reconfigurable family of systems (FoS) designed to maximize joint interoperability, strategic transportability, and commonality of mission roles."[52] It is the core of the Future Force's brigade-sized Unit of Action (UA), comprised of 18 manned and unmanned platforms centered around the Soldier and integrated by a battle command network. FCS will provide Soldiers with significantly enhanced situational awareness, enabling them "to see first, understand first, act first, and finish decisively." An

FCS-equipped Army force will be capable of providing mobile, networked command, control, communication and computer (C4) functionalities; autonomous robotic systems; precision direct and indirect fires; airborne and ground organic sensor platforms; and adverse-weather reconnaissance, surveillance, targeting, and acquisition.

The FCS program is developing network-centric concepts for a multi-mission combat FoS that will be lethal, strategically deployable, self-sustaining and highly survivable in combat. The FCS-equipped Army unit will be capable of adjusting to a changing set of missions, ranging from humanitarian operations to peacekeeping to combat operations. **Figure 15** illustrates how the networked communications subsystem will provide the connectivity for the brigade-sized UA to interact/interface on the battlefield within the FCS FoS and from the Army's FCS platforms to the Unit of Employment (UE), the Joint Force, the Multinational Force, the Legacy Army, and Army Stryker units, as well as government and nongovernmental organizations.

Warfighter Information Network—Tactical (WIN-T): Together, FCS and WIN-T will comprise the Army Future Force's network-centric architecture, under the umbrella of the DoD's Global Information Grid (GIG). WIN-T is the key enabler to execute the NCW capability of the Army's Future Force. It is the "tactical digital communications system that will provide advanced commercial-based networking capabilities to the warfighter," replacing the current Mobile Subscriber Equipment (MSE) and Tri-Services Tactical Communications (TRI-TAC) systems. The WIN-T network will provide enhanced C4ISR capabilities that are mobile, secure, survivable, seamless, and capable of supporting multimedia tactical information systems. The network's capability to support unit task reorganization and real-time retasking of battlefield support elements provides a vital enabler for the conduct of NCO.

As the Army's 3rd Infantry Division prepares for its upcoming deployment to Iraq, it is fielding the Joint Network Transport Capability-Spiral (JNTC-S), a capability that will eventually evolve into WIN-T. In effect, JNTC-S, which will also be fielded to the 101st Airborne Division, the 10th Mountain Division, and the 4th Infantry Division, is an interim system intended to bridge the gap between the legacy Mobile Subscriber Equipment (MSE) and WIN-T.[53]

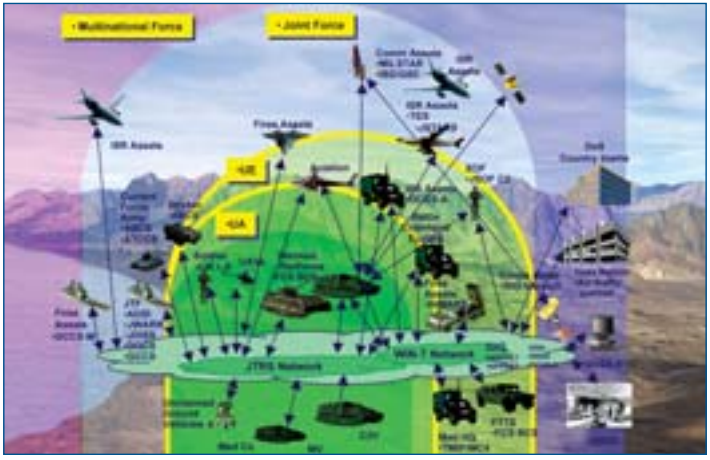


Figure 15: FCS-Enabled Integrated Unit of Action (UA) External Interfaces

Navy and Marine Corps

"The transformation of naval forces is dedicated to greatly expanding the sovereign options available worldwide to the President across the full spectrum of warfare by exploiting our control of the sea. The result of our transformation will be a Navy-Marine Corps Team providing sustainable, immediately employable U.S. combat power as part of a transformed joint force ready to meet any challenge."

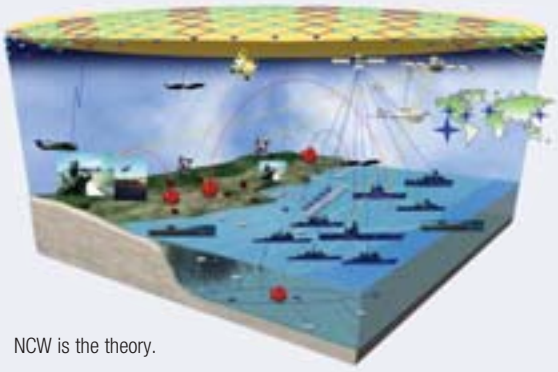
Gordon R. England, Secretary of the Navy,
Admiral Vern Clark, USN, Chief of Naval Operations,
General Michael W. Hagee, USMC, Commandant of the Marine Corps
Foreword, Naval Transformation Roadmap 2003,
April 2004.

Seabasing is the overarching expression of the Navy-Marine Corps Team's shared vision, incorporating the initiatives that will allow the Joint Force to fully exploit one of the United States' asymmetric advantages—command of the sea. Seabasing is the "overarching transformational operating concept for projecting and sustaining naval power and joint forces which assures joint access by leveraging the operational maneuver of sovereign, distributed, and networked forces operating globally from the sea. The sea base of the future will be an inherently maneuverable, scalable aggregation of distributed, networked platforms that enable the global power projection of offensive and defensive forces from the sea … Seabasing unites our capabilities for projecting offensive power, defensive power, command and control, mobility, and sustainment around the world."[54]

Naval Capability Pillars: A series of Navy-Marine Corps capabilities to operationalize Seabasing are being developed through four interdependent and synergistic Naval Capability Pillars (NCP): Sea Shield, Sea Strike, Sea Basing, and FORCEnet. Each NCP represents a broad group of naval capabilities. They summarize the naval tools that will help Joint Force Commanders produce and exploit a discontinuous battlespace within which distributed and sustainable surface, subsurface, air, ground, and space elements form a unified force that assures access and projects both offensive power and defensive capability. FORCEnet will enable these capabilities.

FORCEnet: FORCEnet **(figure 16)** is the operational construct and architectural framework that will provide the Navy-Marine Corps team "with the capability to deliver the persistent and comprehensive surveillance, rapid networked command, and common, accurate battlespace picture necessary to support decision making at a tempo that overwhelms an adversary's capability to react and respond … FORCEnet is the enabling capability for a fully networked naval force, connecting it to the similarly networked joint force that will be linked together by the Internet Protocol (IP)-enabled Global Information Grid." Navy and Marine Corps systems "will be conceived, developed, and implemented as truly joint, integrated capabilities—capable of generating improved coalition effectiveness."

"Implementing the FORCEnet vision will link warfighters ashore, at sea, and in the air into a series of highly integrated distributed services networks that are capable of providing critical operational and tactical information to specified users on a rapid and continuous basis. The 'publish and subscribe' construct for moving data within the network backplane will facilitate greatly improved, shared battlespace awareness, rapid dissemination of the Joint Force Commander's evolving campaign plan/'intent,' and faster passing of information about the enemy from surveillance systems through controllers to ready forces with the right weapons for attacking key targets. FORCEnet enhances naval capabilities to quickly make and execute decisions in the battlespace, to synchronize the activities of widely distributed forces to mass effects on the enemy," and to reduce threats to friendly forces by providing broader situational awareness. "The distributed services and specialized mission applications carried on FORCEnet are as important to future naval combat capabilities as the platforms and weapons they link. Thus, FORCEnet is a critical enabler of naval force transformation."[55]



- NCW is the theory.
- NCO is the concept.
- FORCEnet is the architectural framework to make the theory and concept a reality.

Figure 16: FORCEnet — Enabling Capability for the Fully Networked Naval Force

Air Force

"Our legacy aircraft systems were built with specialized roles and they were very good. But we have limited networking, limited all-weather delivery and limited stand off, and our sensors are only partially integrated … We will network these systems in ways that enable us to find, fix, track, target, engage, and assess in timelines unimaginable just a few years ago. It is our goal to have consistent, persistent intelligence, surveillance, and reconnaissance, and, once a decision to attack is made, we will attack instantaneously."

Dr. James Roche,
Secretary of the Air Force,
The Air Force Transformation Flight Plan,
November 2003.

The Secretary of the Air Force has identified networking and the enhancement of the Air Force's network-centric capabilities as a top priority in the development of the "transformational capabilities" needed to enable the Air Force's six new concepts of operations (CONOPS) and DoD's transformation goals. In *The Air Force Transformation Flight Plan*, the Service's transformation roadmap for 2004 and beyond, the Air Force embraces the key Joint Force Attributes of the *Joint Operations Concepts* (*JOpsC*), including fully integrated, networked, decentralized, and adaptable, and is developing concepts and capabilities to support them.[56]

The first five of 16 transformational capabilities identified by the Air Force that it "cannot achieve today or must be significantly improved to enable the new JOCs, DoD's transformation goals, and the Air Force Vision and CONOPS" are clearly aimed at enabling NCO:

- Seamless joint machine-to-machine integration of all manned, unmanned, and space systems;
- Real-time picture of the battlespace;
- Predictive Battlespace Awareness;
- Ensured use of the information domain via effective information assurance and information operations; and
- Denial of effective C4ISR to adversaries via effective information operations.[57]

In the context of air and space operations, the Air Force believes that the closely related concepts of parallel warfare and effects-based operations (EBO) are "the keys to threat avoidance and applying the right force to the right place at the right time."[58] Network-centric capabilities will enable both.

Parallel Warfare: Parallel warfare refers to the simultaneous attack of carefully selected targets to achieve specific effects, as opposed to attacking targets in a more sequential fashion with the goal of destroying everything on a target list. Until the 1990–91 Gulf War, parallel warfare was very difficult to execute because of the requirement for mass to compensate for a lack of precise weaponry, the large number of assets needed to suppress enemy air defenses, and a general lack of understanding of EBO. The development of low observable "stealthy" platforms, precision weapons, and information operations capabilities, along with a new concept of operations (i.e., EBO), overcame these obstacles and made parallel warfare possible.

Effects-Based Operations: As explained in *The Air Force Transformation Flight Plan*, the main idea of effects-based operations is to design campaign actions based on desired national security outcomes, rather than merely attacking targets to destroy adversary forces. The goal is to understand the effect that is desired in the battlespace and then create that effect more efficiently and effectively. EBO may enable striking fewer targets, using fewer weapons, avoiding enemy threats, mitigating the consequences of enemy action, and limiting the potential for collateral damage and civilian casualties that might occur from a more traditional air campaign. EBO also focuses on combining and coordinating all elements of national power, military and non-military, to achieve its goals by influencing the will and perception of the adversary's decision makers. It requires intelligence analysis that reveals what an adversary relies on to exert influence and conduct operations and the ability to get that intelligence and all other relevant information to the right place at the right time. It also requires the ability to precisely conduct operations in the right order, with a wide range of tools, to include non-lethal weapons and information operations.[59]

Command and Control (C2) Constellation: The centerpiece of the Air Force's NCW implementation efforts is the C2 Constellation initiative **(figure 17)**. The Air Force is transitioning from collecting data through a myriad of independent systems (such as Rivet Joint, AWACS, JSTARS, and space-based assets) to a C2 Constellation capable of providing the Joint Force Commander with real-time, enhanced battlespace awareness. It will provide Ground Moving Target Indicator capabilities along with focused Air Moving Target Indicator capabilities for Cruise Missile

Defense. Additionally, every platform will be a sensor on the integrated network. Regardless of mission function (C2, ISR, shooters, tankers, etc), any data collected by a sensor will be passed to all network recipients. This requires networking all air, space, ground, and sea-based ISR systems, command and control nodes, and strike platforms to achieve shared battlespace awareness and a synergy to maximize the ability to achieve the JFC's desired effects.[60]

Network Centric Collaborative Targeting (NCCT): NCCT is an Advanced Concept Technology Demonstration (ACTD) that will demonstrate a network-centric operating system designed to horizontally integrate air, space, and surface ISR assets at the digital level. By providing a seamless, machine-to-machine interface, this ACTD will improve geo-location accuracy, timeliness, and combat identification of time sensitive targets. With an enhanced wide-band battle management C4ISR network, it will ultimately enable a network-centric, distributed processing environment by leveraging existing sensors, communications, and processing systems to dramatically reduce the time required to detect, identify, locate, and designate fleeting targets. The long-range goal is to expand this capability to additional ISR sensor systems to create a greater network-centric approach to find, fix, and track time-sensitive targets.[61]

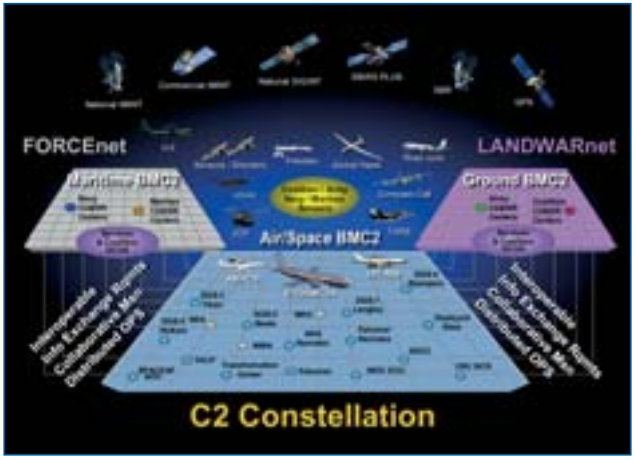


Figure 17: C2 Constellation Interoperability with Maritime and Ground Battle Management Command and Control (BMC2) Systems to Provide Joint BMC2

Allies and Multinational Partners

Around the world, the armed forces of many nations are developing their individual responses to the challenges and opportunities of the Information Age. A growing number of our allies and multinational partners are exploring new technologies and operational concepts in order to develop or enhance the network-centric capabilities of their forces. Some have conducted NCO while working together with U.S. forces in Afghanistan, Iraq, Bosnia, Kosovo, and elsewhere. The partial networking of coalition forces during recent combat (and other multinational military) operations, including OEF and OIF, has helped move NCW and NCO to a central role in the Information Age transformation of military forces around the world.

Significantly, in November 2003, nine NATO nations (Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom, and the United States) agreed to fund a feasibility study on the NATO Networked Enabled Capability (NNEC) as an important step towards NATO's transformation. Subsequently, three others (Belgium, Denmark, and Turkey) joined this effort. This study, which began in January 2004, is to be completed by June 2005. It is being conducted by the NATO Consultation, Command and Control Agency (NC3A) "with the aim of examining issues raised by the network-centric approach … NNEC is based on national and NATO capabilities (tactical and strategic) being networked together in a 'plug and play' fashion as required to support flexible force structures such as the NATO Response Force.[62] The Allied Command Transformation (ACT) has established an integrated product team for NNEC. It is also developing an NNEC Strategic Framework including an overarching NNEC Concept.

By way of example, the network-centric plans and future capabilities of four U.S. allies are summarized below:

Australia: For the Australian Defence Force (ADF), NCW is a means to achieving a more effective warfighting capacity and lies at the heart of the ADF's vision outlined in Force 2020. In the past, the Australian Department of Defence focused primarily on the delivery of engagement or sensor platforms, with minimal attention paid to an underlying networking infrastructure. Many platforms have thus been "stand alone" in their ability to network with other force elements.

In embracing NCW, the ADF has established a concept-led, long-range, capabilities-based planning view (in the context of achieving a joint system of systems). The initial step in regard to NCW is to enhance the ADF's warfighting effectiveness through improved collaboration and ability to share situational awareness. The following initiatives are being explored:

- Establish a network capability that will link engagement systems with sensor and command and control systems and provide the underlying information infrastructure upon which the networked force will be developed. This network will also provide information interoperability with Australia's allies and coalition partners.

- Examine new sensor technologies for their ability to better cue engagement systems. Notable technology areas being examined include UAVs, high-frequency (HF) radar, space-based surveillance, and unattended ground sensors.

- Examine the human dimensions of the networked force and how doctrine, education, and training may need to change.
- Accelerate the process of change and innovation through alternative partnering arrangements with defense industry.

It is the ADF's aim that a well planned and implemented transition to an effective suite of NCW capabilities will enable the conduct of Effects-Based Operations (EBO) as a centerpiece of the Force of 2020.

Canada: The Canadian Forces (CF) have followed international concept development with regards to NCW and EBO quite closely and undertaken a considerable amount of work in these two related fields, both within Canada and with like-minded allies. The CF seeks to maximize the positive utility and transformational benefit of network-related phenomena and an effects-based approach without overlooking their potential limits and adverse consequences.

In order to do so, the CF seeks to maximize network-based interoperability both internally, with other government departments and with allies. In addition, it sees the full attainment of this potential as extending beyond simply the technical and communications challenges, to include all elements of capability, such as doctrine, organization, training and culture, and the widest possible integration of the elements of national power and influence. This commitment was made clear in the most recent annual report of the Chief of Defence Staff:

> *"First, we must transform the way we perceive and think … We are moving from an industrial, hierarchical mode of thinking to a world powered by collaborative human networks. We must learn to think, behave, and act as a node in a collaborative network that includes our warfighters, all three military environments, our civilian colleagues in the department and broader public security portfolio, as well as our allies."*

Moreover, this commitment is reflected at all levels of command within the CF: NCW and EBO inform force development planning at the strategic and joint levels, and amongst the individual services.

As is the case for many of Canada's allies, the resource-related implications of military transformation compel a degree of pragmatism insofar as implementation within the CF is concerned. Near-term opportunities will be exploited and risk will be tolerated; however, transformation is seen as a journey rather than a destination, and evolutionary adaptation will be the norm.

New Zealand: The four capability concepts upon which New Zealand Defence Force (NZDF) force development is based require:

- A knowledge edge force;
- A force tailored for integrated joint operations;
- A multi-mission force capable of tasks ranging from civil emergency response through peacekeeping to combat; and
- A networked force.

There are likely to be few missions or tasks that the NZDF of the future will undertake where it will not be working at some level with other partners, either the military forces of allies and coalition partners or other national agencies in New Zealand. To be effective in its tasks, the future NZDF must be capable of flexible and versatile networking, with the ability to connect seamlessly internally and with a wide range of other forces and agencies.

Networking activity is concentrated, therefore, on achieving interoperability and the identification of standards on which to base national initiatives. NCW in the NZDF is the concept that will drive programs of work aimed at enabling the warfighter.

NCW programs are currently focused on projects to provide the significant enhancement of connectivity out to and between deployed force elements that are needed to support improved national and coalition networking extending from the strategic to tactical levels. Following on, new programs are underway to upgrade information exchange services and capabilities, culminating with the implementation of the NZDF Joint Command and Control System over the 2005–2007 timeframe.

Participation in Joint Warrior Interoperability Demonstration (JWID) and Combined Federated Battle Lab Network (CFBLNet) experimentation provides particular benefit in enabling the development of concepts and frameworks for NCW as well as enhancing the investigation and implementation of individual elements of NCW.

United Kingdom: The most recent United Kingdom (UK) Strategic Defence Review underscored the importance of Network Enabled Capability (NEC) **(figure 18)**. It also lies at the heart of the UK's Joint High Level Operational Concept, which outlines how the UK expects its forces and methods of operation to develop.

The UK is moving from platform-centric planning to a full NEC to exploit effects-based planning and operations, using more adaptable forces, capable of greater precision and rapid deployability. This will change the way the UK plans and executes operations and place different demands on people, equipment, infrastructure, and processes. This evolutionary process has three phases:

- Interconnection: Based on current doctrine, organizations, processes, and equipment with minor organizational changes and equipment enhancements;
- Integration: Drawing on current doctrine, organizations, processes, and equipment with improved capabilities from major organizational change and systems integration, giving greatly improved, shared understanding; and
- Synchronization: Optimal information management and distribution, supporting developed doctrine, organizations, processes, and equipment with agile mission groups formed dynamically with collaborative working enabled by system flexibility.

NEC is based on seven themes:

- Shared Understanding: Covering situational awareness and command intent;
- Full Information Accessibility: Users able to search, manipulate, and exchange relevant information;
- Effects Synchronization: Achieving desired effects through synchronizing activities;
- Agile Mission Grouping: Enabling the dynamic creation/configuration of task-oriented Groups;
- Dynamic Collaborative Working: Enabling agile C2 in a dynamic, continuous, and synchronized manner;
- Resilient Information Infrastructure: Managed coherent information across the battlespace with secure/assured connectivity; and
- Inclusive Flexible Acquisition: Coordinated Government/Industry action to promote rapid technology insertion and an incremental approach to "net-ready platforms."

A vital NEC component is the UK's Network Integration, Test and Experimentation Capability (NITEworks), an experimentation environment to assess the benefits of NEC and the options for its effective and timely delivery, focused on coordinating joint effects and improved targeting.

Figure 18: Network Enabled Capability (NEC)—Heart of the UK's Joint Vision

Conclusions—Network-Centric Warfare in Perspective

"Here at the end of a millennium we are driven to a new era in warfare. Society has changed. The underlying economics and technologies have changed. American business has changed. We would be surprised and shocked if America's military did not. For nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war. Who can make war is changing as a result of weapons proliferation and the fact that the tools of war increasingly are marketplace commodities. By extension, these affect the where, the when, and the how of war."

Arthur K. Cebrowski and John J. Garstka
"Network-Centric Warfare: Its Origins and Future"
U.S. Naval Institute Proceedings, January 1998.

Conclusions—Network-Centric Warfare in Perspective

Towards a Network-Enabled Force: The 1990s

"How can the [U.S.] military not change?" This simple, yet extraordinarily important question was posed six years ago when discussions of network-centric warfare were in their infancy. The answer is abundantly clear today. The U.S. military is changing at an increasingly rapid pace in response to the Information Age and changes in U.S. strategy, the international environment, and technology. Transformation is a vital component of U.S. defense strategy and NCW occupies a central place within the DoD's force transformation process.

Many recognized, as the nation entered the Information Age, that this new age was also influencing change within the U.S. military. However, in the view of some, this change was not occurring fast enough. They observed that a logical model for implementing NCW was already emerging, but it would require a high-performance information grid to provide a backplane for dynamic computing and communications. This information grid would enable the operational architectures of sensor grids and engagement grids. In turn, sensor grids had the potential to generate high levels of battlespace awareness and synchronize awareness with military operations. Engagement grids could then exploit this awareness and translate it into increased combat power for U.S. forces.[63]

Some very promising network-centric capabilities had been developed, experimented with, and tested by U.S. forces by the late 1990s. Many key elements of the information, sensor, and engagement grids were already in place or readily available by that time. At the planning level, the elements of a DoD-wide intranet were emerging. Joint interoperability could be achieved in large measure when all elements of the three grids were compliant with the Joint Technical Architecture (JTA) and the Defense Information Infrastructure Common Operating Environment (DII COE).

The Navy began experimenting with network-centric operations (NCO) during exercises at sea in the late 1980s when the Cooperative Engagement Capability (CEC) system of systems was developed and initially tested. CEC, combining a high-performance sensor grid with a high-performance engagement grid, was "enabled by a shift to network-centric operations." In 1995, the Navy's Seventh Fleet, commanded by then Vice Admiral Archie Clemins, employed rudimentary NCO to

excellent effect during the dangerous Taiwan Straits crisis.[64] CEC reached Initial Operational Capability (IOC) in 1996 after a series of tests and experiments during the early 1990s. Testing and operational evaluations continued in the late 1990s and early 2000s. Today CEC, combined with the Marine Corps' CEC-based Composite Tracking Network, is creating an effective, common network of sensors and weapons that extends the naval air defense capability over sea and shore. Thus, it is an important capability of the Navy-Marine Corps' overall C2 architecture, FORCEnet.[65]

Also in the 1990s, the Army was testing digitization and network-centric concepts and making very significant investments in the development of new warfighting capabilities as it fielded and began to experiment with the first digitized brigade in the 4th Infantry Division at Fort Hood, Texas. Advanced Warfighting Experiments (AWE) were conducted at the National Training Center at Fort Irwin, California, as well as Advanced Concept Technology Demonstrations (ACTD) to demonstrate and test new concepts and technologies. Eventually, the entire 4th Infantry Division became the Army's first digitized division, which presented for the first time an entire division that was truly networked with Force XXI Battle Command Brigade and Below (FBCB2) providing the core capability. It was deployed to Southwest Asia in 2003 for participation in Operation Iraqi Freedom and its aftermath.

Similarly, the Air Force used a combination of Expeditionary Force Exercises (EBX) and ACTDs to explore the potential of networking and digitization. The power of information sharing to enable increased survivability and lethality in the air-to-air mission was substantiated by the Air Force in the mid-1990s during the Joint Tactical Information Distribution Systems (JTIDS) Operational Special Project. Air Force Pilots flying F-15Cs with and without data links clearly demonstrated the power of information sharing enabled by data links. Now the Air Force is developing a series of new CONOPS based on improving network-centric and other transformational capabilities while building the Command and Control (C2) Constellation as described in the previous chapter.

Building Transformational Capabilities in the 21st Century

What about the present and the future of NCW and NCO? NCW as an emerging theory of war is becoming more and more an integral part of how the military is transforming and clearly impacted the development of the Joint Operations Concepts (JOpsC), the Joint Operating Concepts (JOC), and the current Transformation Roadmaps of the Joint Forces Command (JFCOM) and the Services. In short, NCW theory and the governing principles of a network-centric force are guiding, and will likely continue to guide, the development of future warfighting concepts and the development of transformational capabilities within the U.S. Armed Forces.

As shown in this document, great strides have been made in refining NCW theory, documenting the benefits and warfighting advantages of NCW, developing network-centric capabilities, and generally implementing NCW throughout the U.S. Armed Forces in the first few years of the 21st century. Indeed, the most visible and convincing evidence of the validity of NCW theory and the tremendous potential of networked, joint forces (even partially networked joint forces) has been provided by our experience, together with our coalition partners, in Operations Enduring Freedom and Iraqi Freedom from 2001 to the present.

And yet so much remains to be done. Like the force transformation process itself, the development and implementation of NCW capabilities to enable the Joint Force is likely to be a long-term, continuous process with no clear end in sight.

Implementing NCW—Three Cautions

In implementing NCW, no matter how successfully, we must consider that it is nearly impossible to generate certainty on the battlefield with regard to outcomes and consequences. Effects-based operations cannot deliver inviolate cause-effect relations, but they can put the odds on our side. That may be as good as we can get. The multi-sided dynamics of combat defy prediction. NCW is meant to help with this reality, and it does.

Second, the military competition is continuous and no military is as thoroughly studied as our own. As we have become more formidable on the traditional battlefield, potential adversaries have moved to the extremes of terrorism and irregular warfare at one end and weapons of mass destruction (WMD) and catastrophic warfare at the other. Just as the Department must shift its focus to these extremes, so must it work to exploit NCW principles and sources of power there.

Third, over time information technology and networking will become commodities. Everyone will have them. At that point, the advantage will go to those best able to exploit those commodities with new organizations and the ability to rapidly change organizations, new doctrine, the ability to create and discard doctrine rapidly, and the ability to create and assimilate technologies within very short cycle times.

Sources

Ackerman, Robert K. "Iraq War Operations Validate Hotly Debated Theories," *Signal*, July 2003, pp. 31-34.

Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military* (revised). Washington, DC: Department of Defense (DoD) Command and Control Research Program (CCRP), June 2002.

Alberts, David S., John J. Garstka, and Frederick Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised). Washington, DC: DoD CCRP, 2000.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington, DC: DoD CCRP, 2001.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command … Control … in the Information Age*. Washington, DC: DoD CCRP, 2003.

Australian Defence Force, *Enabling Multidimensional Manoeuvre: The Australian Defence Force Network-centric Warfare Concept*. Canberra, Australia: ADO Network-Centric Warfare Conference, May 2003.

Binnendijk, Hans, editor. *Transforming America's Military*. Washington, DC: National Defense University Press, 2002.

Bracken, Paul. "Corporate Disasters: Some Lessons for Transformation," *Joint Forces Quarterly*, Autumn 2002, pp. 83-87.

Cebrowski, Arthur K. "Network Centric Operations and Force Transformation," keynote speech at the Network Centric Warfare 2003 Conference, Arlington, Virginia, 22 January 2003.

Cebrowski, Arthur K. "New Rules, New Era Pentagon Must Embrace Information Age," *Defense News*, October 21-27, 2002, 28.

Cebrowski, Arthur K. "Sea Change," *Surface Warfare*, November-December 1997.

Cebrowski, Arthur K. "The Small, The Fast, and the Many," *NetDefense*, 15 January 2004, p. 10.

Cebrowski, Arthur K. "Transforming Defense," briefing used by the Director, Force Transformation, Office of the Secretary of Defense, March 2003.

Cebrowski, Arthur K. "Transforming Defense," speech to the Heritage Foundation, Washington, DC, 13 May 2003.

Cebrowski, Arthur K. "Transforming Defense," speech at the Center for Naval Analysis (CNA), 20 November 2002.

Cebrowski, Arthur K. and John J. Garstka, "Network-Centric Warfare: Its Origins and Future," *U.S. Naval Institute Proceedings*, Annapolis, Maryland, January 1998.

Cebrowski, Arthur K. and Thomas P.M. Barnett, "The American Way of War," *U.S. Naval Institute Proceedings*, January 2003.

Department of the Navy. *Naval Transformation Roadmap 2003: Assured Access & Power Projection … From the Sea*, Washington, DC, April 2004.

Department of the Navy. *Naval Transformation Roadmap 2004 (Draft)*, Washington, DC, July 2004.

Department of Defense. *Joint Operations Concepts*. Washington, DC: November, 2003.

Department of Defense. *Homeland Security Joint Operating Concept*. Washington, DC, February 2004.

Department of Defense. *Major Combat Operations Joint Operating Concept*, Version 1.10. Washington, DC, 8 June 2004.

Department of Defense. *Network Centric Warfare Report to Congress*. Washington, DC, 27 July 2001.

Department of Defense. *Quadrennial Defense Review Report*. Washington, DC, 30 September 2001.

Department of Defense. *Stability Operations Joint Operating Concept*, Version 1.06. Washington, DC, 8 June 2004.

Department of Defense. *Strategic Deterrence Joint Operating Concept*. Washington, DC, February 2004.

Department of Defense. *Transformation Planning Guidance*, Washington, DC, April 2003.

Director, Office of Force Transformation, Office of the Secretary of Defense. *Military Transformation: A Strategic Approach*. Washington, DC, November 2003.

Director, Office of Force Transformation, Office of the Secretary of Defense. "Network-Centric Operations Case Study: Air-to-Ground," Draft, June 2004. Research performed by Evidence Based Research, Inc. and Science Applications International Corporation.

Director, Office of Force Transformation, Office of the Secretary of Defense. "Network-Centric Operations Case Study: Naval Special Warfare Group One (NSWG-1)," Draft, June 2004. Research performed by Evidence Based Research, Inc. and Booz-Allen Hamilton, Inc.

Director, Office of Force Transformation, Office of the Secretary of Defense. "Network-Centric Operations Case Study: The Stryker Brigade Combat Team," Draft, May 2004. Research performed by RAND National Defense Research Institute.

Director, Office of Force Transformation, Office of the Secretary of Defense and UK Ministry of Defense. "Network-Centric Operations Case Study: U.S./UK Coalition Combat Operations during Operation Iraqi Freedom," Draft, June 2004. Research performed by Evidence Based Research, Inc. and PA Consulting.

Echevarria II, Antulio J. *Toward An American Way of War*. Carlisle Barracks, Pennsylvania: Strategic Studies Institute, Army War College, March 2004.

Evans, Michael. "From Kadesh to Kandahar: Military Theory and the Future of War," *The Naval War College Review*, Summer 2003, Vol. LVI, No. 3, article 6.

Fairbanks, Walter P. *Information Superiority: What Is It? How to Achieve It?* Cambridge, Massachusetts: Center for Information Policy Research, Harvard University, June 1999.

Franks, General (U.S. Army, Ret.) Tommy. "Impact of the Network on Operation Iraqi Freedom," a special presentation at the Network-Centric Warfare 2004 conference, Washington, DC, 22 January 2004.

Garstka, John J. "Network-Centric Warfare: An Overview of Emerging Theory," *PHALANX: The Bulletin of Military Operations Research*, Volume 33 No. 4, December 2000.

Garstka, John J. "Network-Centric Warfare Offers Warfighting Advantage," *Signal*, May 2003, pp. 58-60.

Graham, Janice M. "'Learning from Transforming the Commercial Sector," *Joint Force Quarterly*, Autumn 2002, pp. 88-92.

Handel, Michael I. *Masters of War: Classical Strategic Thought* (3rd revised and expanded edition). London: Frank Cass, 2001.

Hsu, Emily. "Division Expects 'Quantum Leap' in Communications Technologies in Iraq," *Inside the Army*, 23 August 2004.

Kaufman, Paula. "Network-Centric Warfare – The Key to the Revolution in Military Affairs," *IEEE Spectrum*, July 2002.

Keeter, Hunter C. "Network Centric Warfare Aims to Translate Information Superiority into Combat Advantage," *Sea Power*, March 2004, pp. 12-14.

Kime, Patricia. "OFT Case Studies Aim to Codify Tenets of Networked Operations," *Sea Power*, March 2004, pp. 21-22.

Myers, Richard B. "Understanding Transformation," *U.S. Naval Institute Proceedings*, February 2003.

NATO. "Signing Ceremony to Initiate a Study on NATO Network Enabled Capability (NNEC), NATO HQ, Brussels, 13 November 2003," NATO Press Release (2003), 12 November 2003.

Office of Force Transformation, Office of the Secretary of Defense. *Network Centric Operations Conceptual Framework, Version 1.0*, November 2003.

Office of Force Transformation, Office of the Secretary of Defense. *Network Centric Operations Conceptual Framework, Version 2.0 (Draft)*, June 2004.

Onley, Dawn S. "Net-Centric Approach Proven in Iraq," *Government Computer News*, Vol. 23, No. 10, May 2004.

President of the United States. *The National Security Strategy of the United States of America*. Washington, DC, September 2002.

Robinson, Jr., Clarence A. "Military Marches Toward Agility," *Signal*, May 2003, pp. 17-20.

Scott, William B. and David Hughes. "Nascent Net-Centric War Gains Pentagon Toehold," *Aviation Week & Space Technology*, 27 January 2003.

Secretary of Defense. *Annual Report to the President and the Congress*. Washington, DC, 15 August 2002.

Smith, Jr., Edward A. *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. Washington, DC: DoD CCRP, November 2002.

Smith, Jr., Edward A. "Network-Centric Warfare: What's the Point?" *Naval War College Review*, Winter 2001.

U.S. Air Force. *The Air Force Transformation Flight Plan*, Washington, DC, November 2003.

U.S. Air Force. *The U.S. Air Force Transformation Flight Plan 2004*, Washington, DC, July 2004.

U.S. Army. *United States Army 2003 Transformation Roadmap*, Washington, DC, November 2003.

U.S. Army. *2004 Army Transformation Roadmap*, Washington, DC, 4 August 2004.

U.S. Joint Forces Command. *Joint Lessons Learned: Operation Iraqi Freedom Major Combat Operations, Coordinating Draft*, Norfolk, Virginia, 1 March 2004.

U.S. Joint Forces Command. *Joint Transformation Roadmap*, 3 November 2003 (Draft).

U.S. Joint Forces Command. *Joint Transformation Roadmap*, Norfolk, Virginia, 30 July 2004.

Notes

[1] For an understanding of the nature, purposes, and direction of defense transformation, including force transformation, see the *Transformation Planning Guidance* document approved by Secretary of Defense Donald Rumsfeld in April 2003. See also *Military Transformation: A Strategic Approach*, a document approved by the Director, Office of Force Transformation, OSD, in November 2003.

[2] Vice Admiral (Ret.) Arthur K. Cebrowski, Director, Office of Force Transformation, interview with Frank Swofford, *Defense AT&L*, March-April 2004.

[3] John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage," *Signal*, May 2003, p. 58.

[4] Edward A. Smith, Jr., *Effects-Based Operations: Applying Network-Centric Warfare in Peace, Crisis, and War*, Washington, DC: DoD CCRP, 2002, p. 108.

[5] Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings*. Annapolis, Maryland: January 1998.

[6] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised). Washington, DC: DoD CCRP, 2000.

[7] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, Washington, DC: DoD CCRP, 2001. David S. Alberts, *Information Age Transformation: Getting to a 21st Century Military* (revised), Washington, DC: DoD CCRP, June 2002.

[8] Edward A. Smith, Jr., *Effects-Based Operations: Applying Network-Centric Warfare in Peace, Crisis, and War*, Washington, DC: DoD CCRP, 2002.

[9] See the final chapter, "The Emerging Way of War," in *Military Transformation: A Strategic Approach*, a document published by the Director, Office of Force Transformation, OSD in November 2003.

[10] These four basic tenets of NCW were initially set forth in *Network-Centric Warfare: Department of Defense Report to Congress*, 27 July 2001.

[11] Department of Defense. *Network-Centric Warfare Report to Congress*. Washington, DC, 27 July 2001, pp. ii-iii.

[12] The "Key Elements of Strategy" for implementing NCW in the Department were presented in a briefing, "Defense Transformation and Network-Centric Warfare," by Vice Admiral (Ret.) Arthur K. Cebrowski at the Network Centric Warfare 2004 conference on 22 January 2004, Washington, DC. They have also been presented in numerous briefings by John Garstka, Office of Force Transformation, 2002-2004. See also the foldout brochure, "Network-Centric Warfare: Creating a Decisive Warfighting Advantage," published by the Director, Force Transformation, Spring 2004.

[13] Frederick C. Mish, Editor in Chief, *Webster's Ninth New Collegiate Dictionary.* New York: Merriam-Webster, Inc., 1990, p. 1223.

[14] David B. Guralnik, Editor in Chief, *Webster's New World Dictionary of the American Language*, Second College Edition. New York: Prentice Hall, 1986, p. 1475.

[15] *The Art of War* by Sun Tzu and *On War* by Carl von Clausewitz are widely regarded as classic theoretical works on war. Other well known theorists of war include Niccolo Machiavelli *(The Art of War)*, Baron Antoine-Henri Jomini *(The Art of War)*, Mao Tse-tung *(Selected Military Writings of Mao Tse-tung)*, and Alfred Thayer Mahan *(The Influence of Sea Power Upon History)*.

16 According to the DoD's *Joint Operations Concepts (JOpsC)* document approved by the Secretary of Defense in November 2003, "Information Superiority is an imbalance in one's favor in the information domain with respect to an adversary. The power of superiority in the information domain mandates that the United States fight for it as a first priority even before hostilities begin." See *JOpsC*, p. 17. For an in-depth, scholarly examination of the term "information superiority," how information superiority can be achieved, and whether it can be measured by assessing the performance of C4ISR systems during military operations, see Walter P. Fairbanks, *Information Superiority: What Is It? How to Achieve It?* Cambridge, Massachusetts: Center for Information Policy Research, Harvard University, June 1999.

17 Michael I. Handel, *Masters of War: Classical Strategic Thought* (3rd revised and expanded edition). London: Frank Cass, 2001, pp. xx-xxiii. For a recent critique of "the new American way of war" and emerging NCW theory, see pp. 12-18 of Lieutenant Colonel Antulio J. Echevarria II, U.S. Army. *Toward An American Way of War*. Carlisle Barracks, Pennsylvania: Strategic Studies Institute, Army War College, March 2004. LTC Echevarria describes the underlying concepts of the current American way of war as "a polyglot of information-centric theories such as network-centric warfare, rapid decisive operations, and shock and awe." These concepts focus "on 'taking down' an opponent quickly rather than finding ways to apply military force in the pursuit of broader political aims. Moreover, the characteristics of the U.S. style of warfare—speed, jointness, knowledge, and precision—are better suited for strike operations than for translating such operations into strategic success. "

18 Michael Evans, "From Kadesh to Kandahar: Military Theory and the Future of War," *The Naval War College Review*, Summer 2003, Vol. LVI, No. 3, article 6.

19 "Impact of the Network on Operation Iraqi Freedom," a special presentation by General Tommy Franks, USA (Ret.) at the Network-Centric Warfare 2004 conference on 22 January 2004, Washington, DC.

20 Office of Force Transformation, OSD, *Network Centric Operations Conceptual Framework, Version 1.0*, November 2003, pp. 10-11. See also *Network Centric Operations Conceptual Framework, Version 2.0 (Draft)*, June 2004, pp. 24-25.

21 John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage," *Signal*, May 2003, p. 58-59.

22 Ibid., pp. 59-60.

23 Captain Dane Acord, Commander, B Company, 2nd Battalion, 8th Infantry, 2nd Brigade Combat Team, 4th Infantry Division (Mechanized), DCX-1. (The acronym, FBCB2 refers to the Army's Force XXI Battle Command Brigade and Below system.)

24 The Joint Operations Concepts is "an overarching definition of how the future Joint Force will operate across the entire range of military operations. It is the unifying framework for developing subordinate joint operating concepts, joint functional concepts, enabling concepts, and integrated capabilities." Department of Defense, *Joint Operations Concepts*, Washington, DC, November 2003, p. 5.

25 Ibid., pp. 15-18.

26 Department of Defense, *Transformation Planning Guidance*, Washington, DC, April 2003, p. 15.

27 Department of Defense. *Major Combat Operations Joint Operating Concept, Version 1.10*. Washington, DC, 8 June 2004, pp. 12, 14-15.

28 "Impact of the Network on Operation Iraqi Freedom," keynote address by General Tommy Franks, USA (Ret.) at the Network-Centric Warfare 2004 conference on 22 January 2004, Washington, DC.

[29] Robert K. Ackerman, "Iraq War Operations Validate Hotly Debated Theories," *Signal*, July 2003, p. 31-34.

[30] Remarks by Vice Admiral (Ret.) Arthur K. Cebrowski, Director, OFT at the Network-Centric Warfare 2004 conference on 22 January 2004, Washington, DC.

[31] Remarks by Vice Admiral (Ret.) Arthur K. Cebrowski, Director, OFT, at the Defense Writers Group, 23 April 2003.

[32] Office of Force Transformation, OSD, *Network Centric Operations Conceptual Framework, Version 2.0 (Draft)*, June 2004, p. 2. See also *Network Centric Operations Conceptual Framework, Version 1.0*, November 2003.

[33] Ibid. p. 4.

[34] Ibid. pp. 78-80. See also Director, Office of Force Transformation, "Network Centric Operations Case Study: The Stryker Brigade Combat Team (Draft.)" May 2004.

[35] Ibid. pp. 76-77. See also Director, OFT, "Network Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom (Draft)." June 2004.

[36] Ibid. pp. 74-76. See also Director. OFT, "Network Centric Operations Case Study: Air-to-Ground" (Draft). Vienna, VA, June 2004.

[37] Ibid. pp. 83-88. See also Director, OFT, "Network Centric Operations Case Study: Naval Special Warfare Group One (NSWG-1), Draft." June 2004.

[38] "Impact of the Network on Operation Iraqi Freedom," a special presentation by General Tommy Franks, USA (Ret.) at the Network-Centric Warfare 2004 conference on 22 January 2004, Washington, DC.

[39] "Situational Awareness in OIF via FBCB2 – Blue Force Tracking: A Preview of Future Battle Command," a briefing by Colonel Nick Justice, USA and Colonel Curtis McCoy, USA at the Network-Centric Warfare 2004 conference on 22 January 2004, Washington, DC.

[40] "Net-Centric is an approach to exploitation of advancing technology that moves from an approach based on applications standards to one based on data standards—that is, providing users the ability to access applications and services that make sense to them through a Web-enabled space, while simultaneously moving toward a Web-enabled user community in which each members can provide and access data." "About Net-Centricity" page on the Horizontal Fusion website: http://www.horizontalfusion.dod.mil/vision.

[41] U.S. Air Force, *The Air Force Transformation Flight Plan*, Washington, DC, November 2003, p. B-4.

[42] U.S. Joint Forces Command, *Joint Transformation Roadmap*, 21 January 2004, p. 10.

[43] Ibid., pp. 10-11.

[44] Ibid., p. 12.

[45] Ibid.

[46] The 2003 Service Transformation Roadmaps and the Joint Transformation Roadmap prepared by USJFCOM were submitted to the Director of Force Transformation in the fall of 2003 and forwarded to the Secretary of Defense in early 2004. (Subsequent Roadmaps will be approved by the Service Secretaries.) The 2004 Service and Joint Transformation Roadmaps were submitted to the Director of Force Transformation in July 2004, but have not yet been reviewed by the Secretary of Defense.

47 U.S. Army, *2003 United States Army Transformation Roadmap*, Washington, DC, November 2003, pp. 1-5, 1-6. The *2004 Army Transformation Roadmap (ATR)* "updates the *2003 ATR* and describes the execution of Army transformation strategy in the context of evolving security challenges, continuing high demand for operational forces, and lessons learned from recent operations." See 2004 ATR, 4 August 2004, p. ii.

48 U.S. Army, *2004 ATR*, 4 August 2004, p. 56.

49 Department of Defense, *Joint Operations Concepts*, Washington, DC, November 2003, pp. 15-18.

50 *2003 United States Army Transformation Roadmap*, p. 1-7.

51 Ibid. pp. 1-12, 1-13. The *2004 ATR* states that "the Future Force is founded on six main operational themes," one of which is "networked-enabled Battle Command." See *2004 ATR*, 4 August 2004, p. 55.

52 Ibid., p. B-3.

53 Emily Hsu, "Division Expects 'Quantum Leap' in Communications Technologies in Iraq," *Inside the Army*, 23 August 2004.

54 Department of the Navy, *Naval Transformation Roadmap 2003: Assured Access & Power Projection … From the Sea*, Washington, DC, April 2004, p. 2. For an updated discussion of the Joint Seabasing concept, see Chapter II, "Transformational Concepts," of the *Naval Transformation Roadmap 2004 (Draft)*, Washington, DC, July 2004, pp. 6-8.

55 Ibid. pp. 3-4, 63-64. For an updated discussion of the FORCEnet Naval Capability Pillar (NCP), see pp. 68-85 of the *Naval Transformation Roadmap 2004 (Draft)*, Washington, DC, July 2004, pp. 6-8.

56 U.S. Air Force, *The Air Force Transformation Flight Plan*, Washington, DC, November 2003, pp. 17-18, 45.

57 *The U.S. Air Force Transformation Flight Plan 2004*, Washington, DC, July 2004, p. ES-6. See also *The Air Force Transformation Flight Plan*, Washington, DC, November 2003, p. 45.

58 Ibid, p. 6. See also *The Air Force Transformation Flight Plan*, Washington, DC, November 2003, p. 6.

59 Ibid.

60 *The Air Force Transformation Flight Plan*, Washington, DC, November 2003, p. B-6.

61 Ibid., p. B-7.

62 NATO, "Signing Ceremony to Initiate a Study on NATO Network Enabled Capability (NNEC), NATO HQ, Brussels, 13 November 2003," NATO Press Release (2003) 135, 12 November 2003.

63 Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings*. Annapolis, Maryland: January 1998.

64 Ibid. By taking advantage of the capabilities of the Global Network Initiative (GNI) he had developed and implemented while commanding the Seventh Fleet, Admiral Clemins and his subordinates reduced their planning timelines from days to hours. This "order of magnitude change" suggested to Clemins and others who had witnessed it that "something very fundamental" was happening.

65 Department of the Navy, *Naval Transformation Roadmap 2003: Assured Access & Power Projection … From the Sea*, Washington, DC, April 2004.

Director, Force Transformation, Office of the Secretary of Defense,
1000 Defense Pentagon, Washington, DC 20301-1000
www.oft.osd.mil

Date of Publication: January 5, 2005

Cleared for public release by Department of Defense
Office of Freedom of Information and Security Review, 05-S-0235

This publication is available through the Government Printing Office. For ordering information, call 202.512.1800 or write the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. For GPO publications online access, go to their Web site at: http://www.access.gpo.gov/su_docs/sale.html.